EXHIBIT 2

US7373515B2	OVHcloud (“The Accused System”)
3. In a system wherein both a PIN of a user authorized to access a network resource and a first key of an asymmetric key pair generally unique to a personal communications device of the authorized user are maintained by an authentication authority in association with an identifier such that each of the PIN and the first key are retrievable based on the identifier, a method performed by the authentication authority whereby the authorized user gains access to the network resource from an access authority, the method comprising the steps of:	U2F architecture is a system wherein both a PIN (e.g., password) of a user (e.g., online service user) authorized to access a network resource (e.g., online service) and a first key (e.g., U2F security key i.e. U2F authenticator) of an asymmetric key pair generally unique to a personal communications device (e.g., PC, mobile, Laptop etc.) of the authorized user are maintained by an authentication authority (e.g., U2F server with database) in association with an identifier such that each of the PIN (e.g., password) and the first key (e.g., U2F security key i.e. U2F authenticator) are retrievable based on the identifier, a method performed by the authentication authority (e.g., U2F server with database) whereby the authorized user gains access to the network resource from an access authority (e.g., web server with web application). The accused system recommends 2-factor authentication using FIDO U2F compliant security key at its website. Universal 2nd Factor (U2F) is an open authentication standard that strengthens and simplifies two-factor authentication (2FA) using specialized USB or NFC devices. The ("Fast Identity Online”) FIDO Alliance hosts the standardization. A user registers a U2F compliant device at registration stage. The user logs in with a username and password as before and presents a second factor device when the web service prompts it as shown in the figure below.

EXHIBIT 2

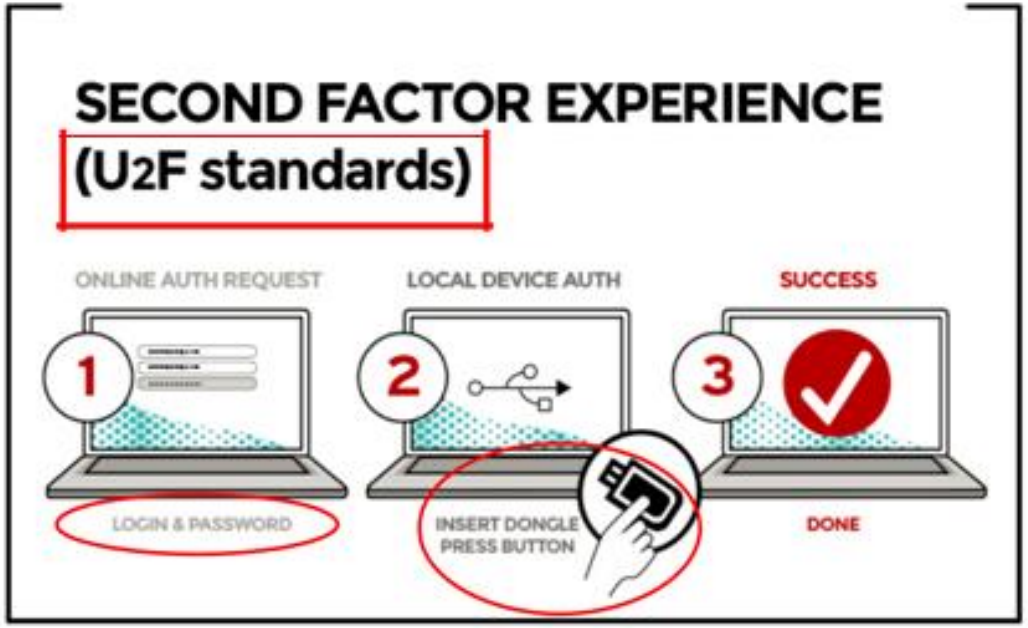
	 https://fidoalliance.org/specifications/

EXHIBIT 2

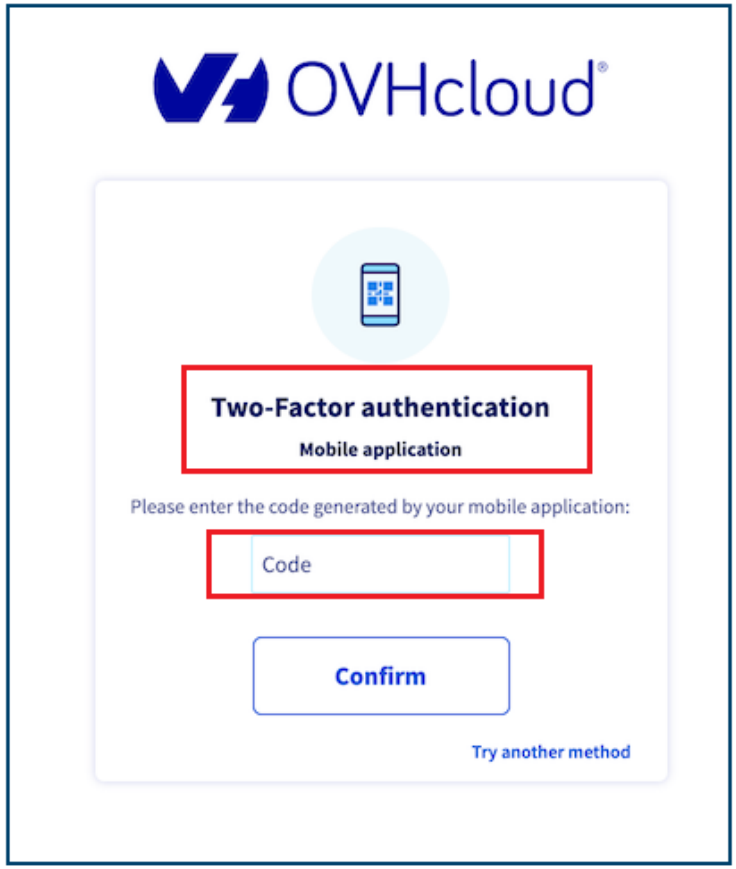
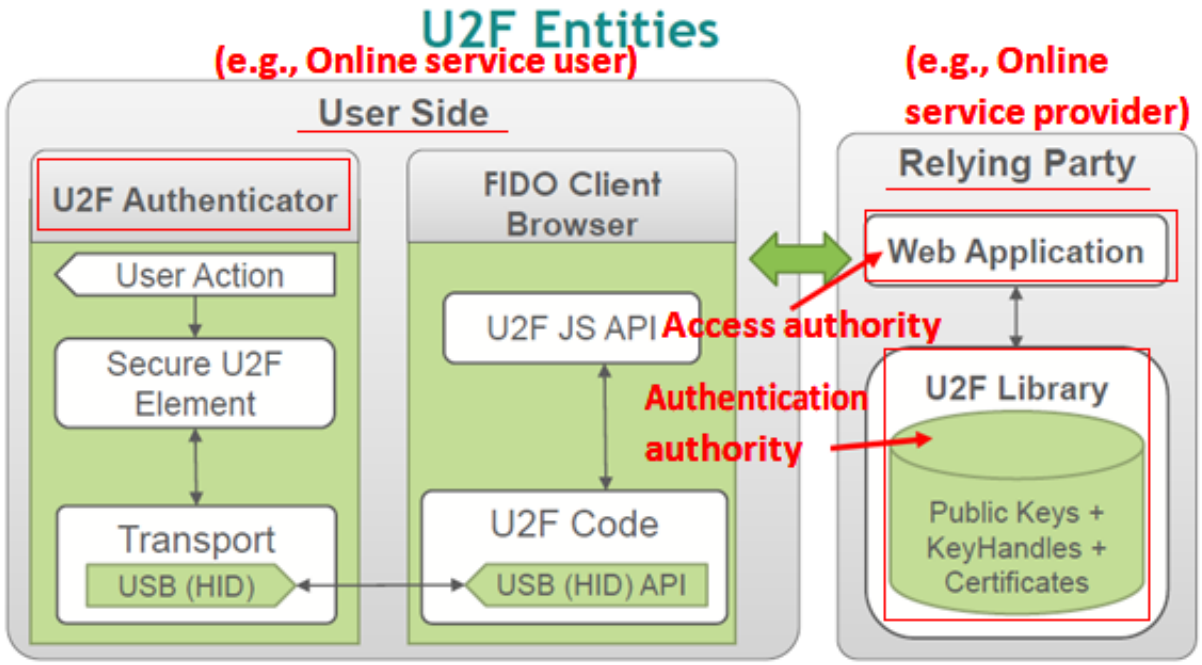
	To test if two-factor authentication has been set up correctly, log out of the OVHcloud Manager c attempt to log back in. If, after entering your password, you are taken to a screen like the one be successfully set up two-factor authentication.  https://support.us.ovhcloud.com/hc/en-us/articles/115001825710-How-to-Use-Two-Factor-Authentication

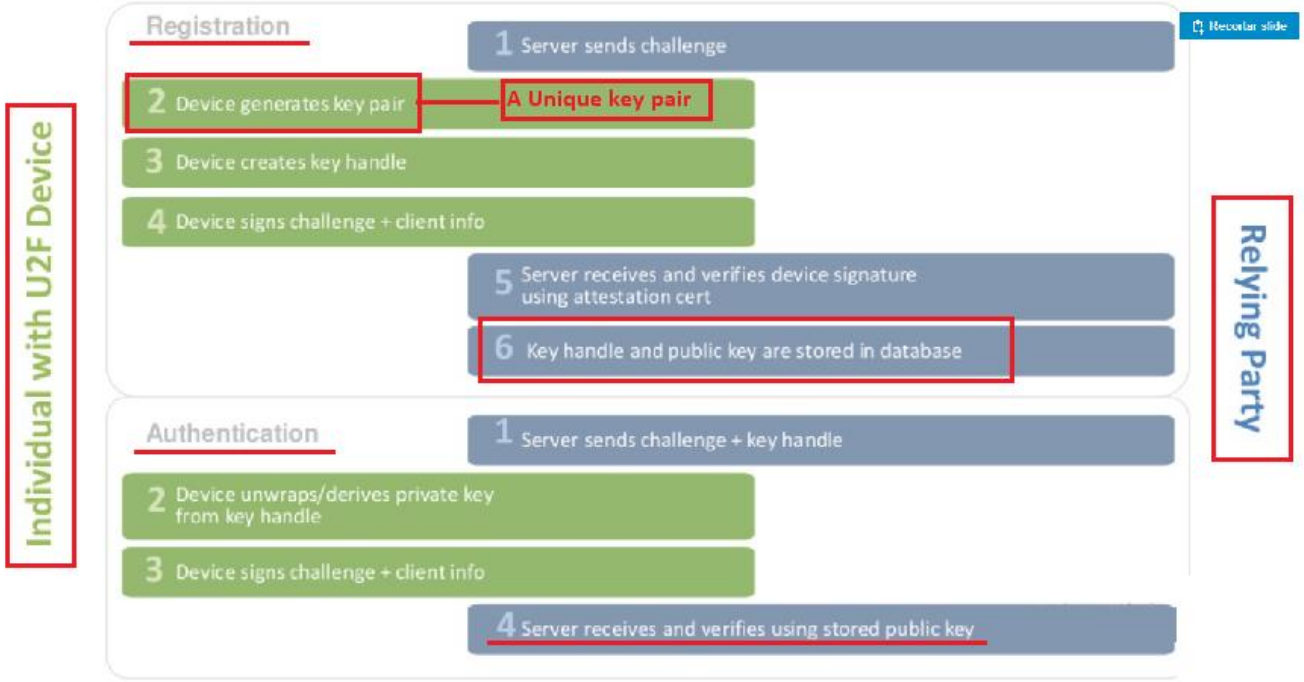
EXHIBIT 2



https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial

To use a U2F device in 2-factor authentication, a user (e.g., Individual with U2F device) has to register the U2F device with an authentication authority in the relying party. In the registration stage, the U2F device generates a unique key pair (A public key and a private key) and a key handle and sends the public key (e.g., a first key) with the handle to the authentication authority in the relying party to store the them in its database of the relying party. The key pair is used to authenticate a suspected user by the authentication authority in the authentication stage.

EXHIBIT 2



https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial

The following figure shows U2F database in the authentication authority in the relying party (e.g., online service provider) after the registration. The authentication authority maintains the public key (=a first key) of the key pair and the key handle generated by the U2F device and an identifier (=user_id), and the password (=a PIN) associated with it in its database. The U2F security key (authenticator) owned by the user maintains the private key of the key pair and the key handle (not shown).

EXHIBIT 2

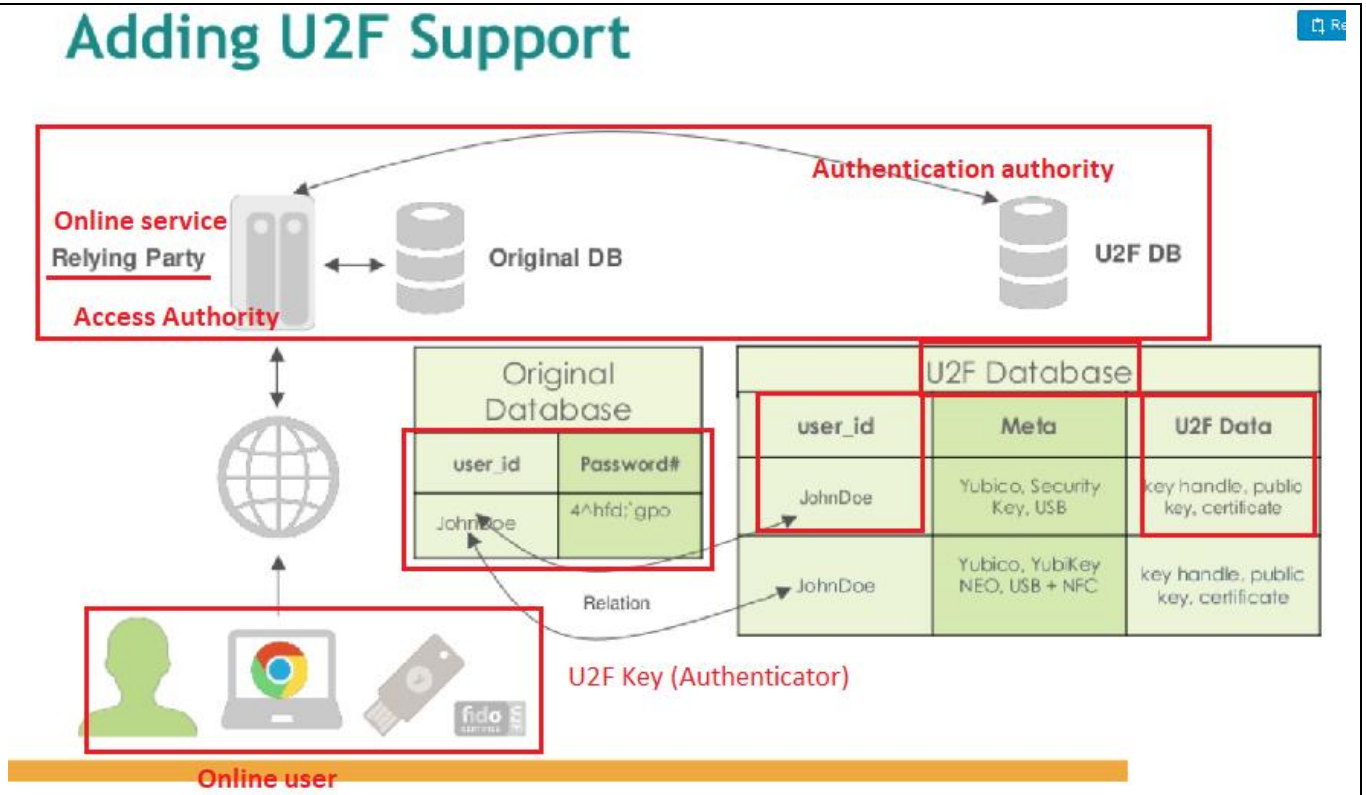
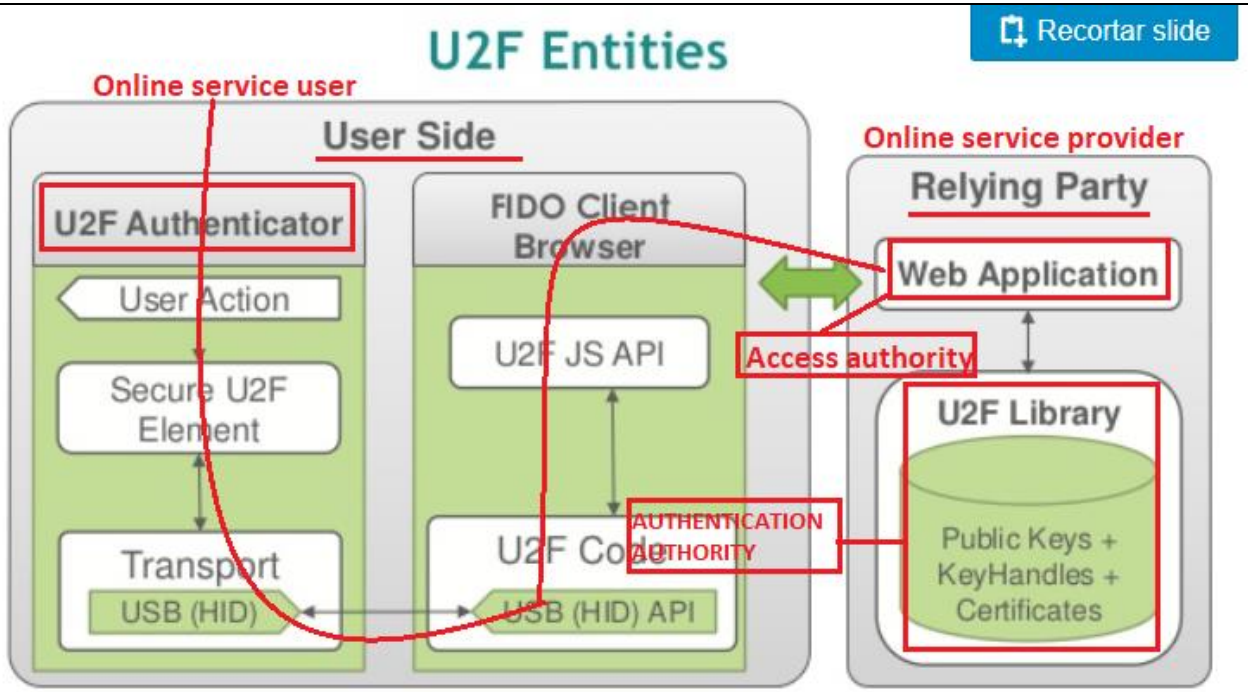
	 https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial
(a) with respect to a suspect user seeking to gain access to the network resource from the access authority, receiving a challenge request from the access authority in association with an identifier;	The accused system practices a method of receiving a challenge request from the access authority in association with an identifier with respect to a suspect user (e.g., Online service user) seeking to gain access to the network resource (e.g., Online service like accused system) from the access authority (e.g., accused system's server). Note that the relying party (e.g., online service provider) comprises an access authority and an authentication authority.

EXHIBIT 2



https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial

If a suspected user with a U2F security key (authenticator) attempts to log in an online service, the web server (=the access authority) in the relying party requests a verification of the user associated with the user-ID and the password and requests a challenge request to the authentication authority to verify the user's U2F security key. In other words, the authentication authority receives the challenge request from the web server (=access authority) with user_id (= an identifier).

EXHIBIT 2

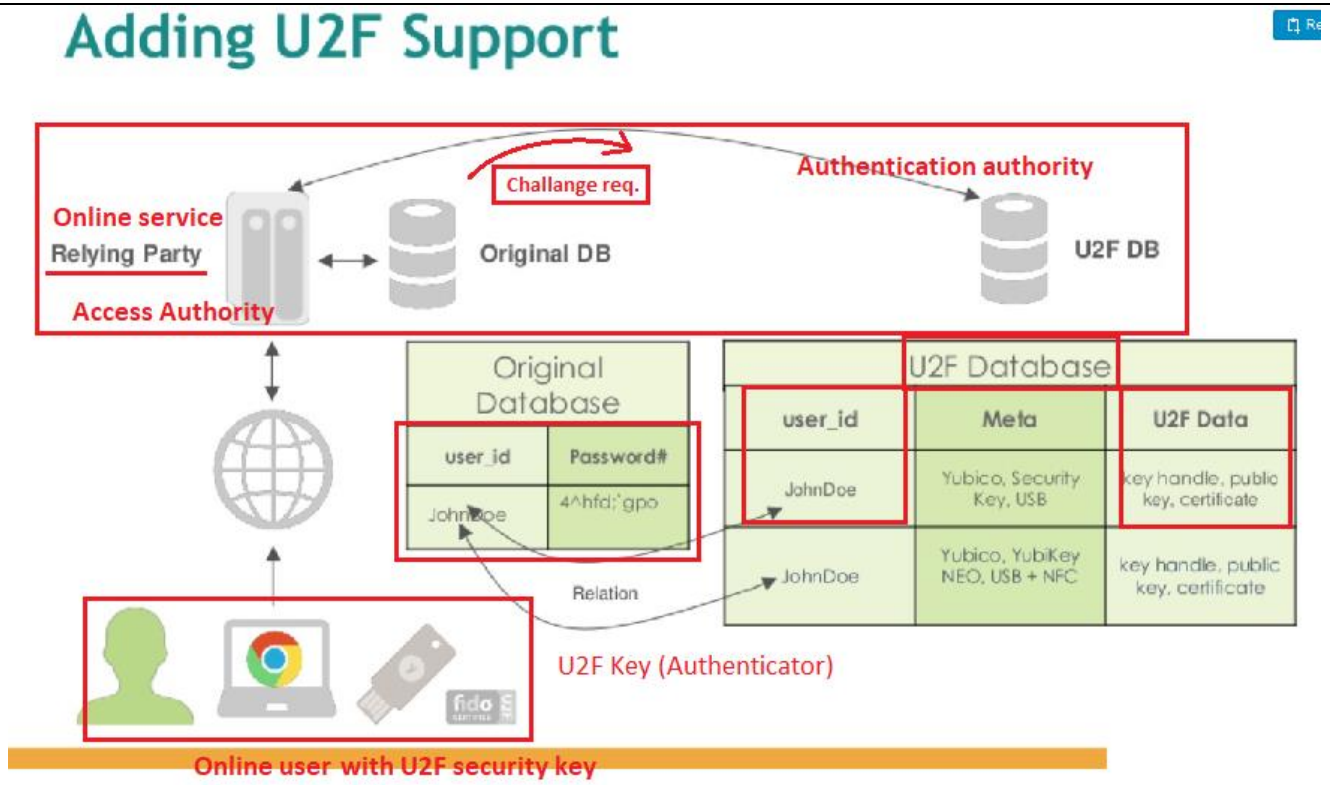
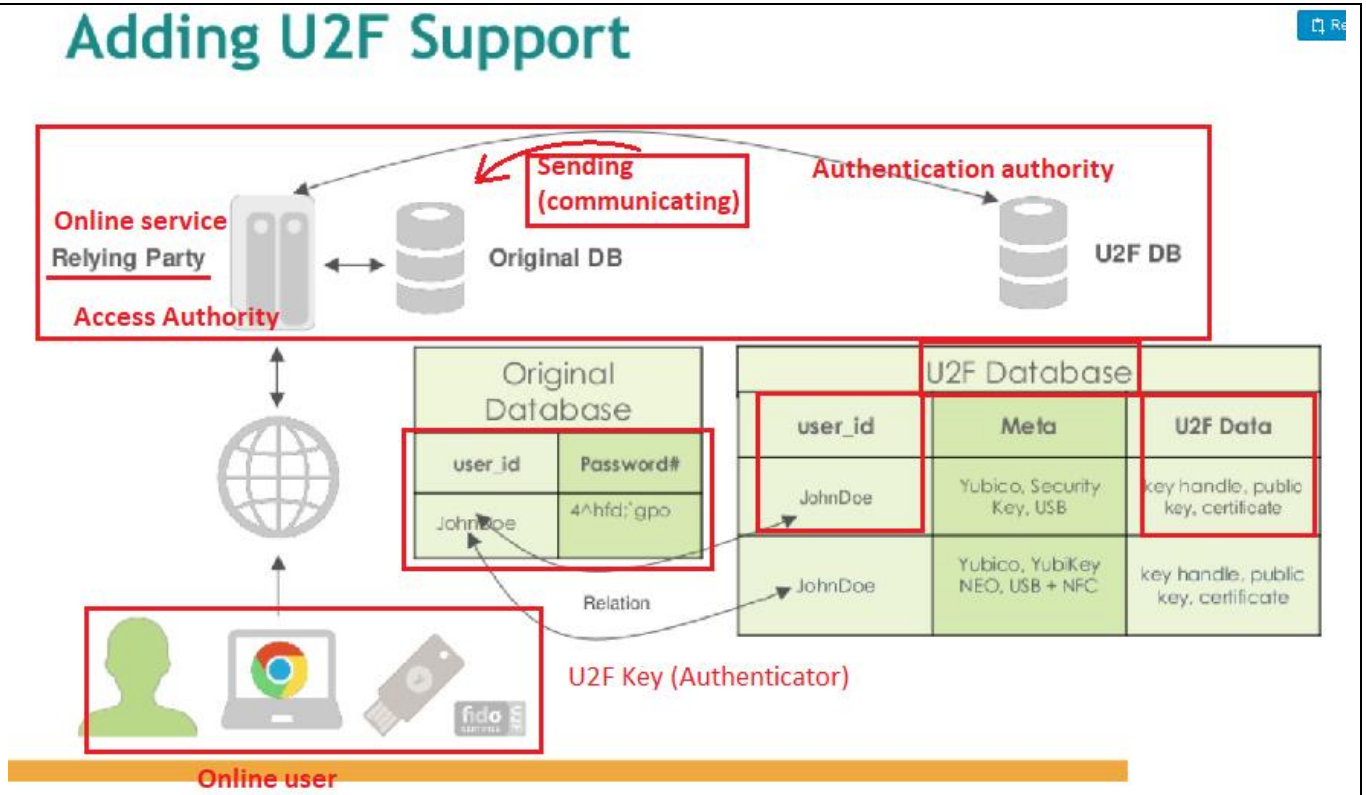
	 https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial
(b) in response to the challenge request, communicating a challenge to the access authority;	The accused system practices communicating a challenge to the access authority (e.g., web server) in response to the challenge request. The authentication authority in the relying party (e.g., online service) sends (=communicates) a challenge to the access authority so that the access authority can send it to the user's U2F authenticator (See the challenge following).

EXHIBIT 2



https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial

FIDO U2F standard describes the steps where the relying party sends a challenge to the U2F authenticator (i.e., U2F security key) via the FIDO Client/Browser. This means that the access authority (e.g., web server) receives the challenge from the authentication authority as described on the previous page.

EXHIBIT 2

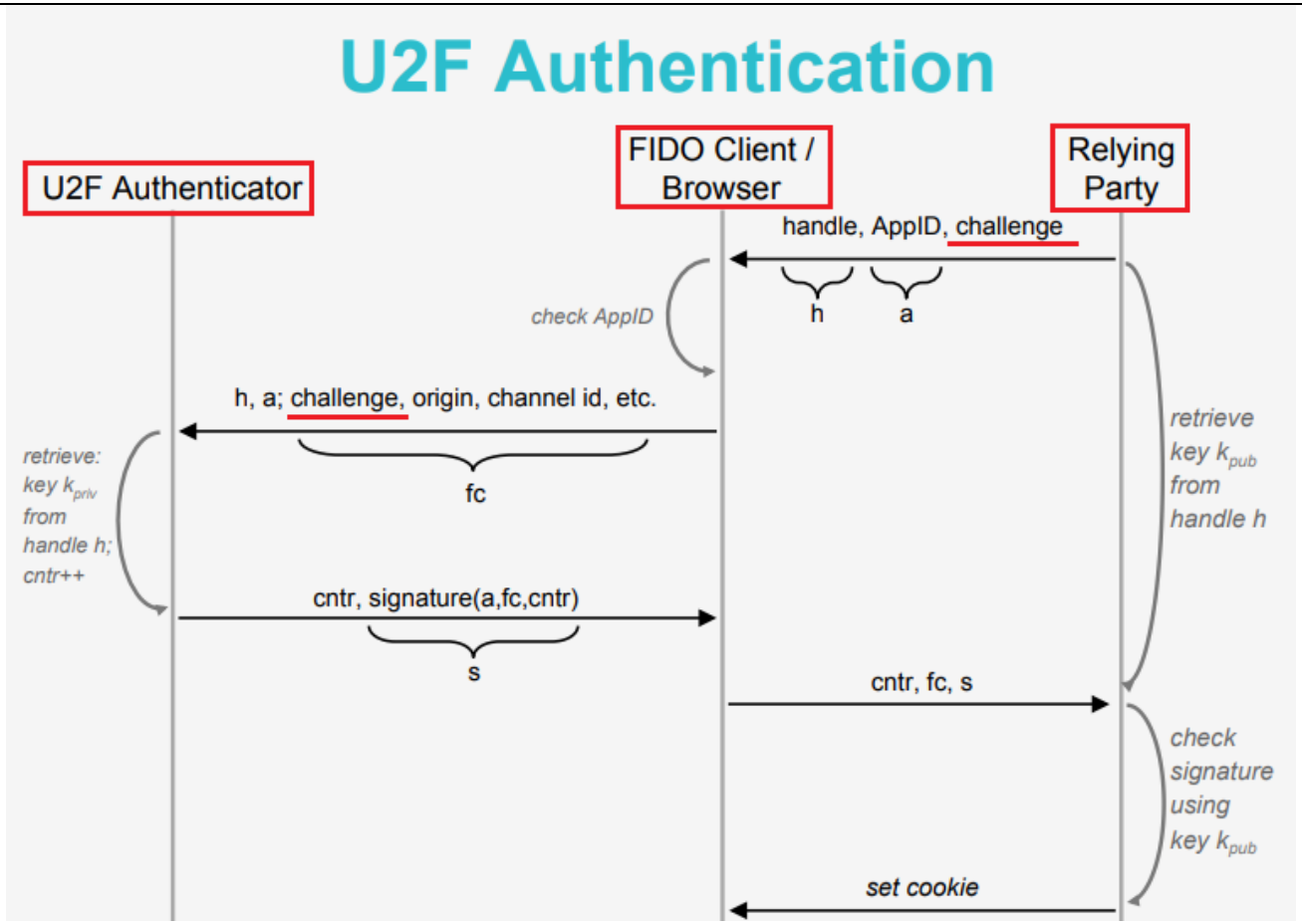
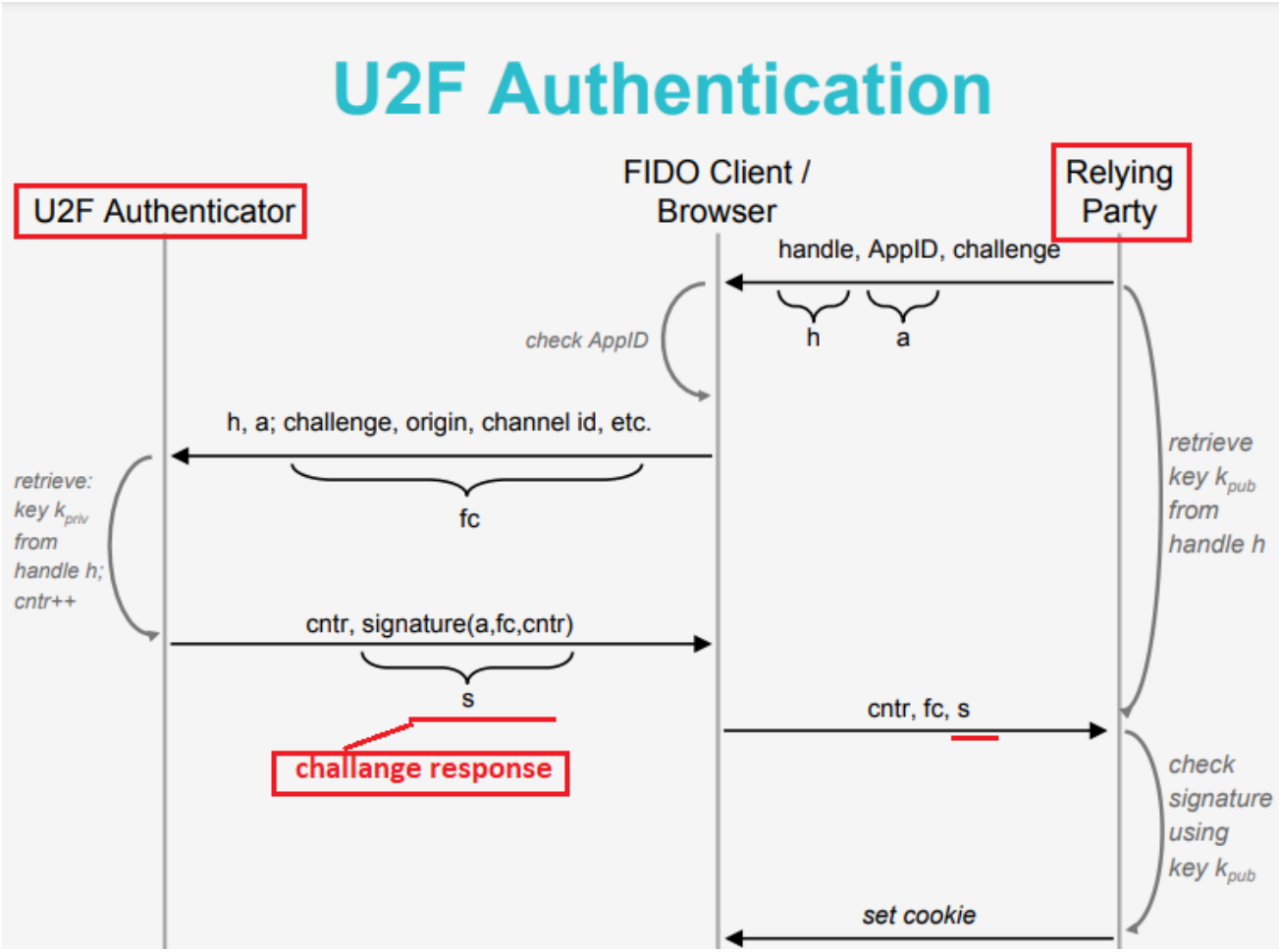
	 https://fidoalliance.org/assets/downloads/FIDO-U2F-UAF-Tutorial-v1.pdf
(c) receiving from the access authority a challenge response and the identifier; and	The accused system practices receiving from the access authority a challenge response and the identifier. Upon receiving the challenge from the access authentication authority, the U2F authenticator processes it and sends the challenge response in the form of signature to the replying party via the FIDO

EXHIBIT 2

client/browser. Therefore the authentication authority receives the challenge response and associated identifier via the access authority (e.g., web server).



https://fidoalliance.org/assets/downloads/FIDO-U2F-UAF-Tutorial-v1.pdf

EXHIBIT 2

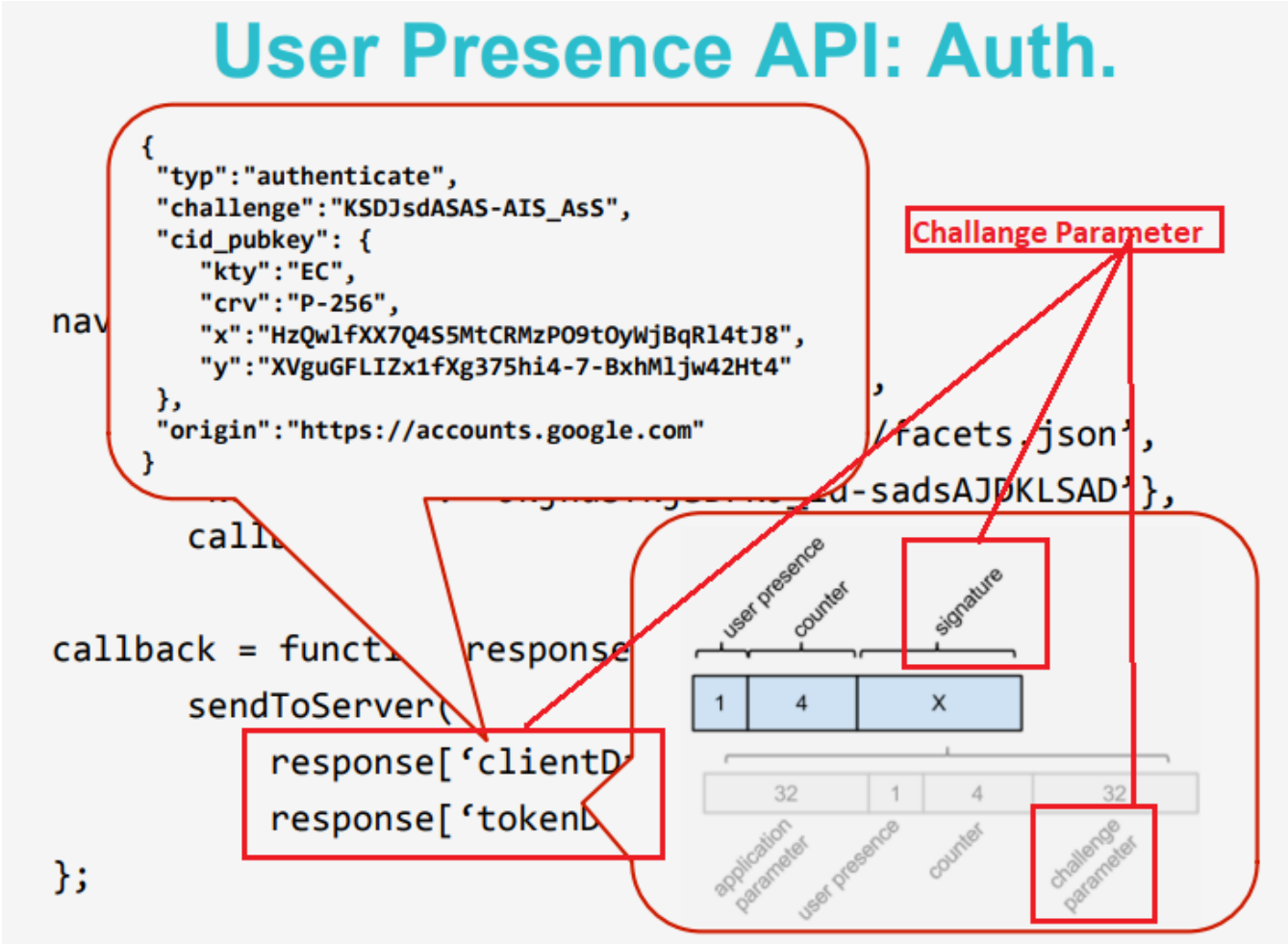
	The following figure shows that the signature (s) in the response comprises the challenge parameter [32 bytes]. The access authority must tell the source of response with the identifier to the authentication authority so that the authentication authority can verify the account and its U2F key (not shown).  https://fidoalliance.org/assets/downloads/FIDO-U2F-UAF-Tutorial-v1.pdf

EXHIBIT 2

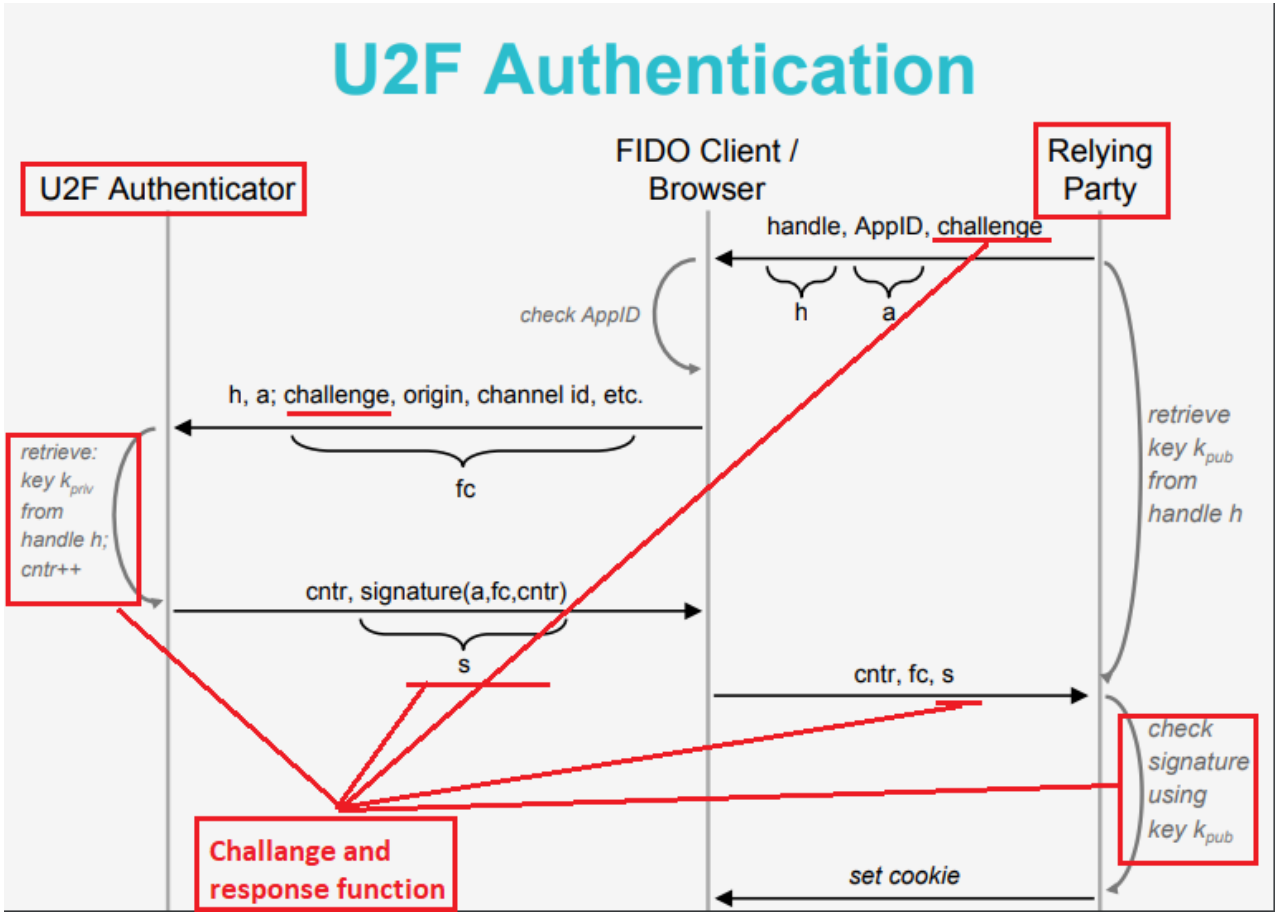
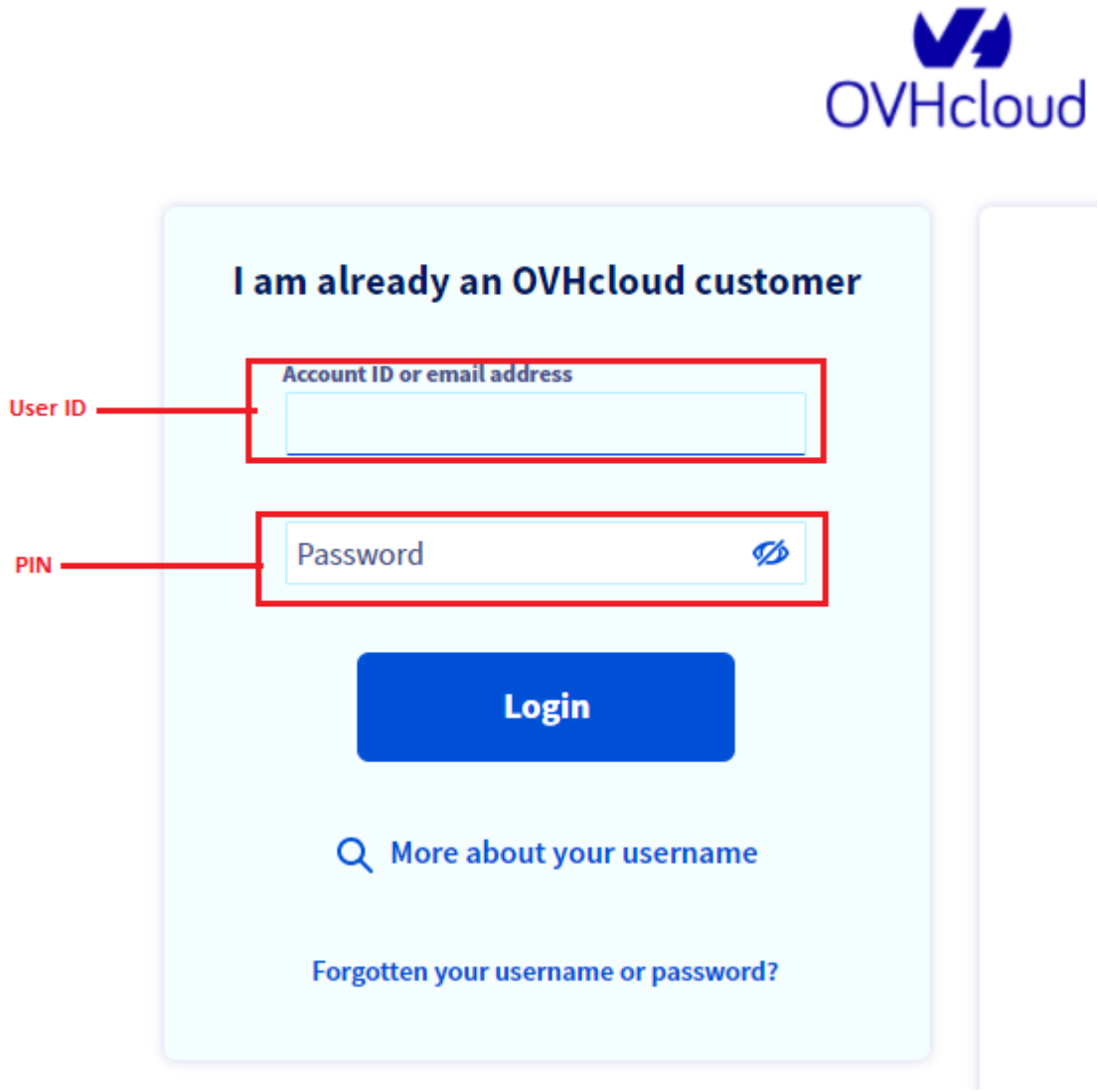
(d) authenticating the identifier by comparing the challenge response to a function of, (i) the challenge;	The accused system practices authenticating the identifier by comparing the challenge response to a function of the challenge. The authentication authority (in the relying party) verifies the identifier by using the challenge and response function.  https://fidoalliance.org/assets/downloads/FIDO-U2F-UAF-Tutorial-v1.pdf

EXHIBIT 2

(ii) the PIN maintained by the authentication authority in association with the identifier; and	The accused system practices authenticating the identifier by comparing the challenge response to a function of the PIN (e.g., password) maintained by the authentication authority (e.g., U2F server with database) in association with the identifier (e.g., associated user ID). The authentication authority in the replying party like accused system also uses the password (=which is equal to a PIN) associated with user ID (=the identifier).

EXHIBIT 2



https://www.ovh.com/auth/?action=gotomanager&from=https://www.ovh.co.uk/&ovhSubsidiary=GB

EXHIBIT 2

	PIN and password are synonyms according to the description of '515 patent shown below. Furthermore, as used herein, "PIN," "passcode," and "password" each broadly refers to a shared secret used for authentication purposes and all are considered synonyms herein, with none intended to imply any particular syntax of the secret itself. The use of "asymmetric key pair" refers to https://patentimages.storage.googleapis.com/0d/08/49/2d86aa8d80d268/US7373515.pdf
(iii) the first key maintained by the authentication authority in association with the identifier.	The accused system practices authenticating the identifier by comparing the challenge response to a function of the first key (e.g., Public key Kpub) maintained by the authentication authority (e.g., U2F server with database in relying party) in association with the identifier. The authentication authority in the relying party verifies the signature received from the U2F authenticator associated with the identifier by decrypting the signature (s) with Kpub which is the public key (=the first key). If the challenge response is decoded successfully with the public key (=the first key) by the authentication authority, the U2F authenticator responds to the challenge is a trusted key.

EXHIBIT 2

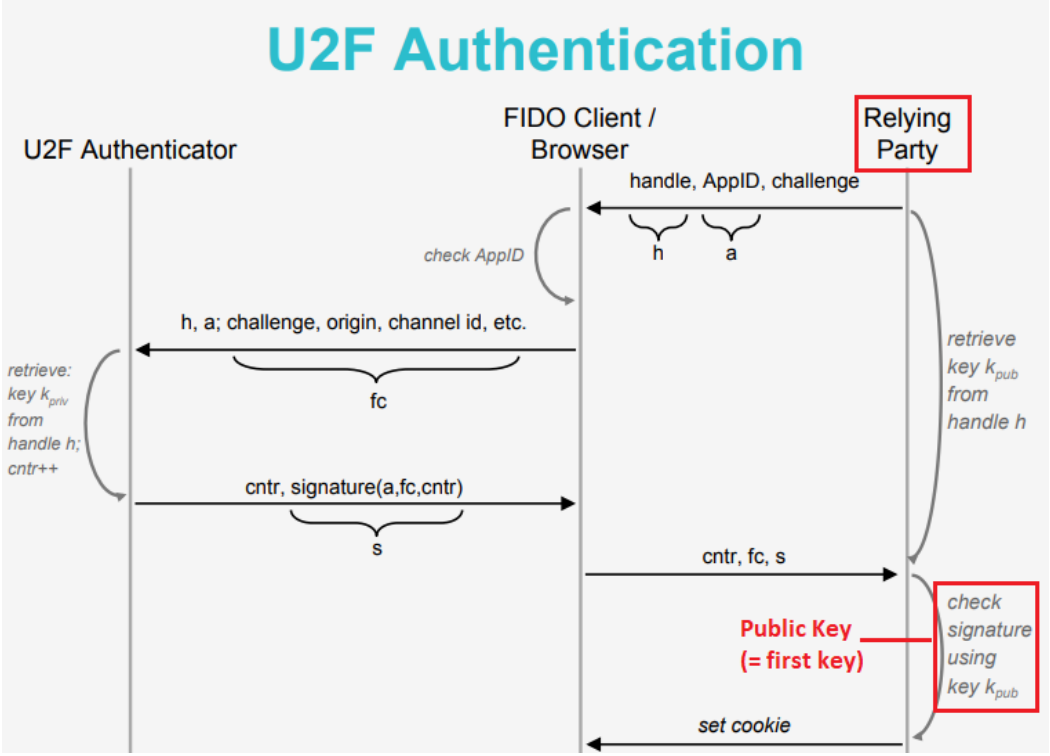
	 https://fidoalliance.org/assets/downloads/FIDO-U2F-UAF-Tutorial-v1.pdf
20. A method of granting access to a suspect user seeking to access a network resource, comprising the steps of:	The accused system practices a method of granting access to a suspect user (e.g., Online service user) seeking to access a network resource (e.g., Online service like accused system). The accused system recommends 2-factor authentication using FIDO U2F compliant security key at its website. Universal 2nd Factor (U2F) is an open authentication standard that strengthens and simplifies two-factor authentication (2FA) using specialized USB or NFC devices. The ("Fast Identity Online") FIDO Alliance hosts the standardization. A user registers a U2F compliant device at registration stage. The user logs in with a username and password as before and presents a second factor device when the web service prompts it as shown in the figure below.

EXHIBIT 2

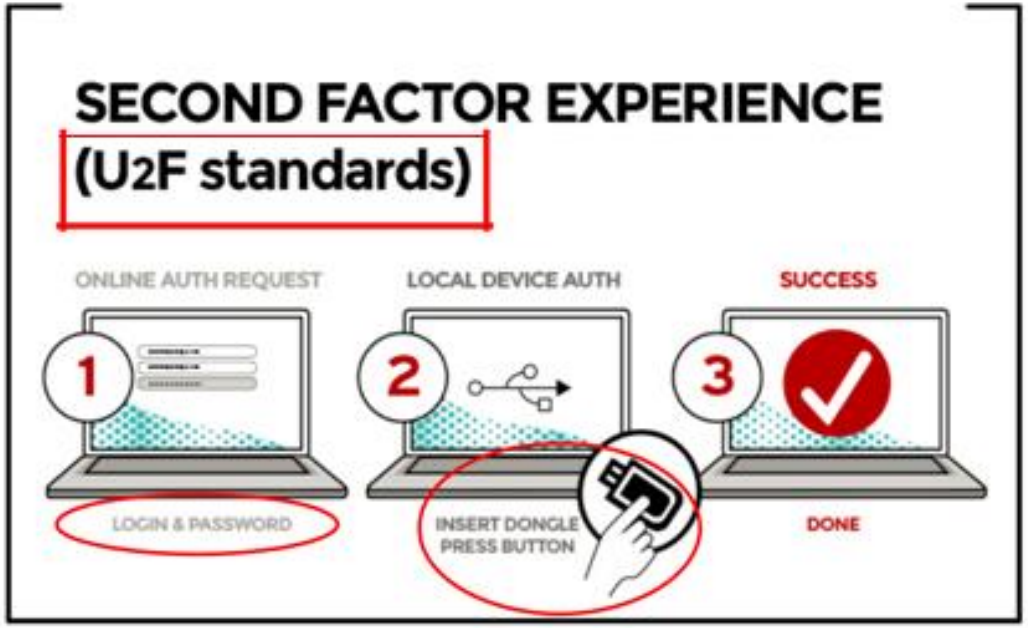
	 https://fidoalliance.org/specifications/

EXHIBIT 2

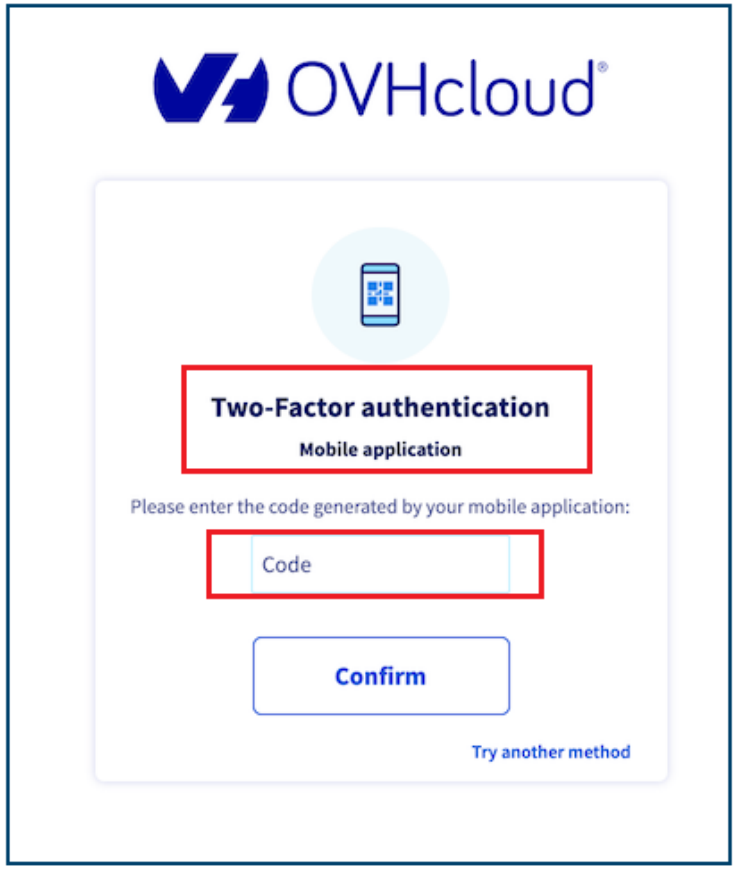
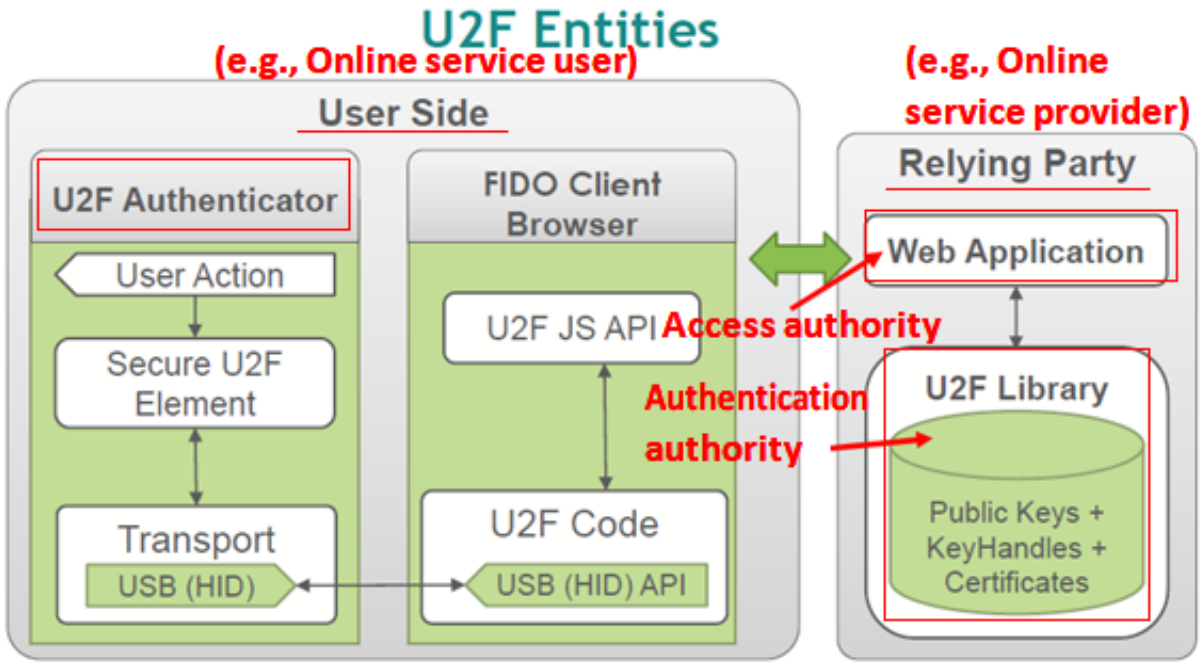
	To test if two-factor authentication has been set up correctly, log out of the OVHcloud Manager c attempt to log back in. If, after entering your password, you are taken to a screen like the one be successfully set up two-factor authentication.  https://support.us.ovhcloud.com/hc/en-us/articles/115001825710-How-to-Use-Two-Factor-Authentication

EXHIBIT 2



https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial

To use a U2F device in 2-factor authentication, a user (e.g., Individual with U2F device) has to register the U2F device with an authentication authority in the relying party. In the registration stage, the U2F device generates a unique key pair (A public key and a private key) and a key handle and sends the public key (e.g., a first key) with the handle to the authentication authority in the relying party to store them in its database of the relying party. The key pair is used to authenticate a suspected user by the authentication authority in the authentication stage.

EXHIBIT 2

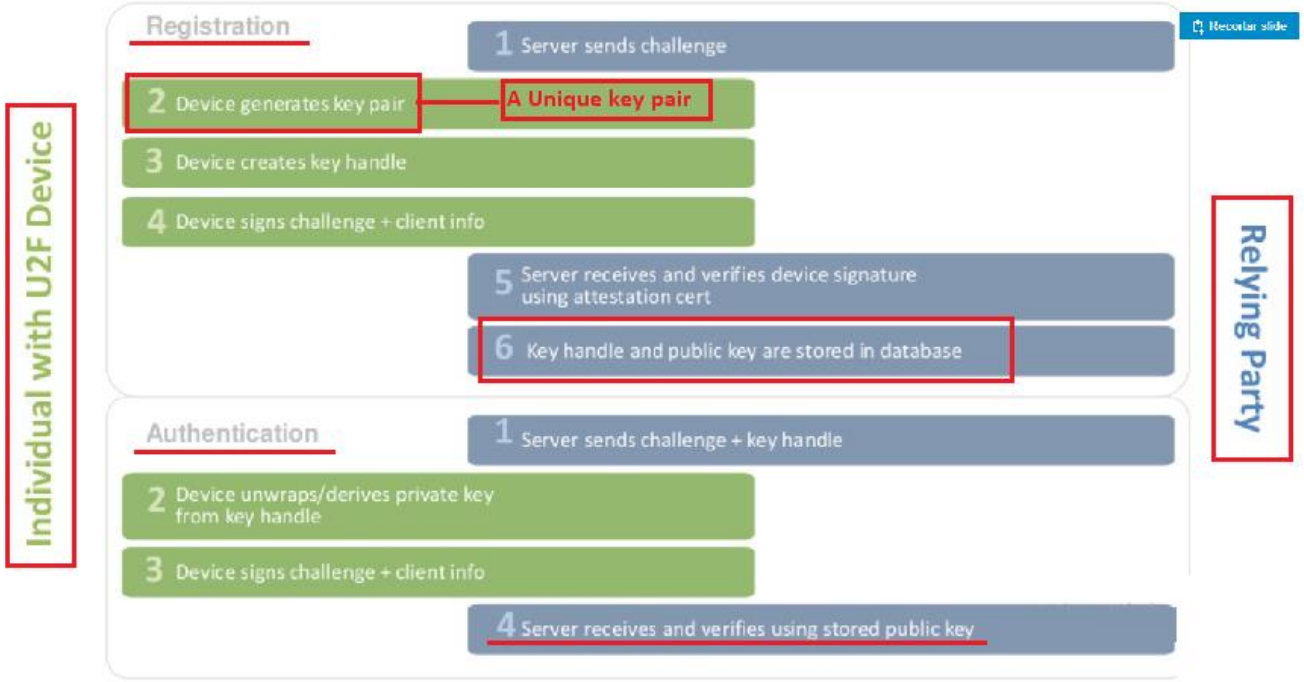
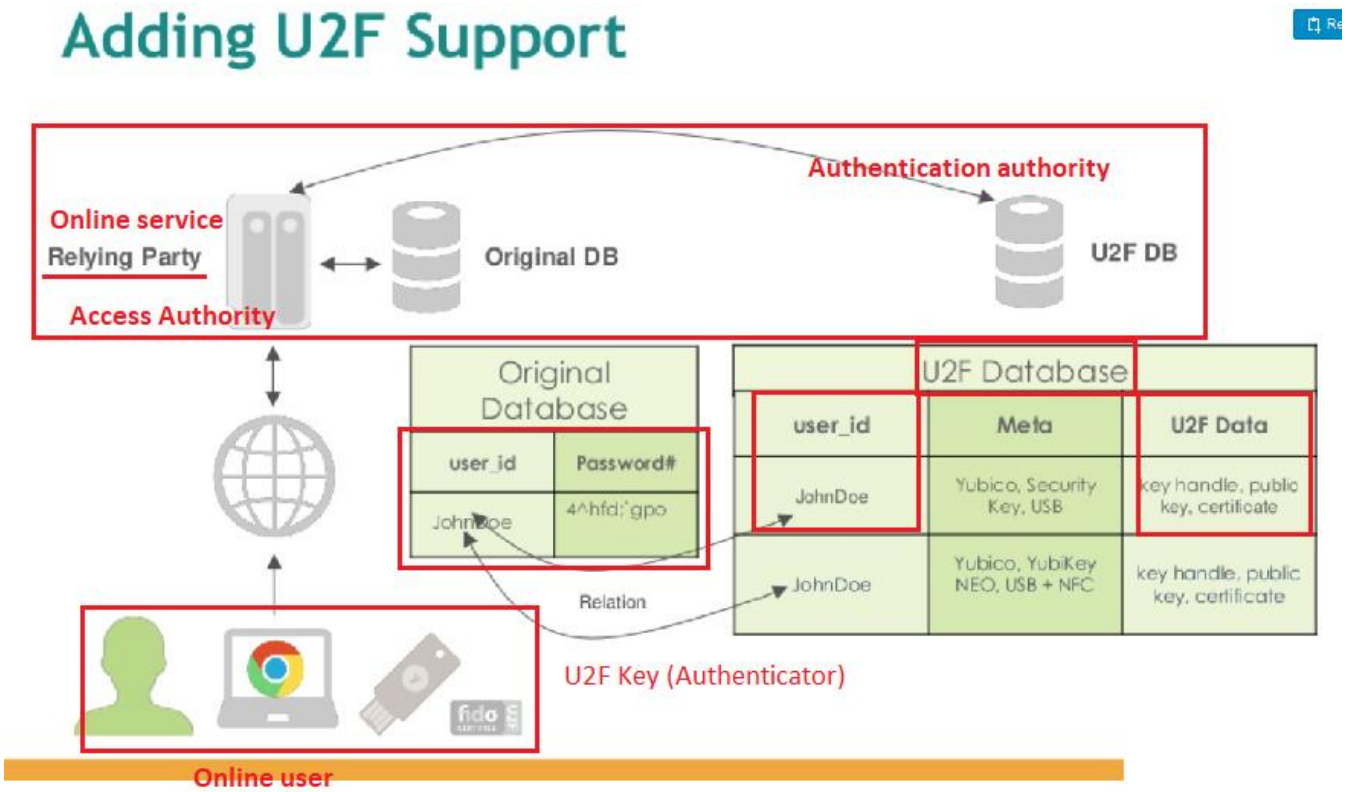
	 https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial
(a) first, (i) maintaining credentials of the authorized user such that the credentials are retrievable based on the user ID,	The authentication authority of the accused system practices maintaining credentials (e.g., PIN of a user, key pair and user ID) of the authorized user such that the credentials are retrievable based on the user ID. U2F architecture is a system wherein both a PIN (e.g., password) of a user (e.g., online service user) authorized to access a network resource (e.g., online service) and a first key (e.g., U2F security key i.e. U2F authenticator) of an asymmetric key pair generally unique to a personal communications device (e.g., PC, mobile, Laptop etc.) of the authorized user are maintained by an authentication authority (e.g., U2F server with database) in association with an identifier such that each of the PIN (e.g., password) and the first key (e.g., U2F security key i.e. U2F authenticator) are retrievable based on the identifier.

EXHIBIT 2

	The following figure shows U2F database in the authentication authority in the relying party (e.g., online service provider) after the registration. The authentication authority maintains the public key (=a first key) of the key pair and the key handle generated by the U2F device and an identifier (=user_id), and the password (=a PIN) associated with it in its database. The U2F security key (authenticator) owned by the user maintains the private key of the key pair and the key handle (not shown).



https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial

Note that the relying party (e.g., online service provider) comprises an access authority and an authentication authority.

EXHIBIT 2

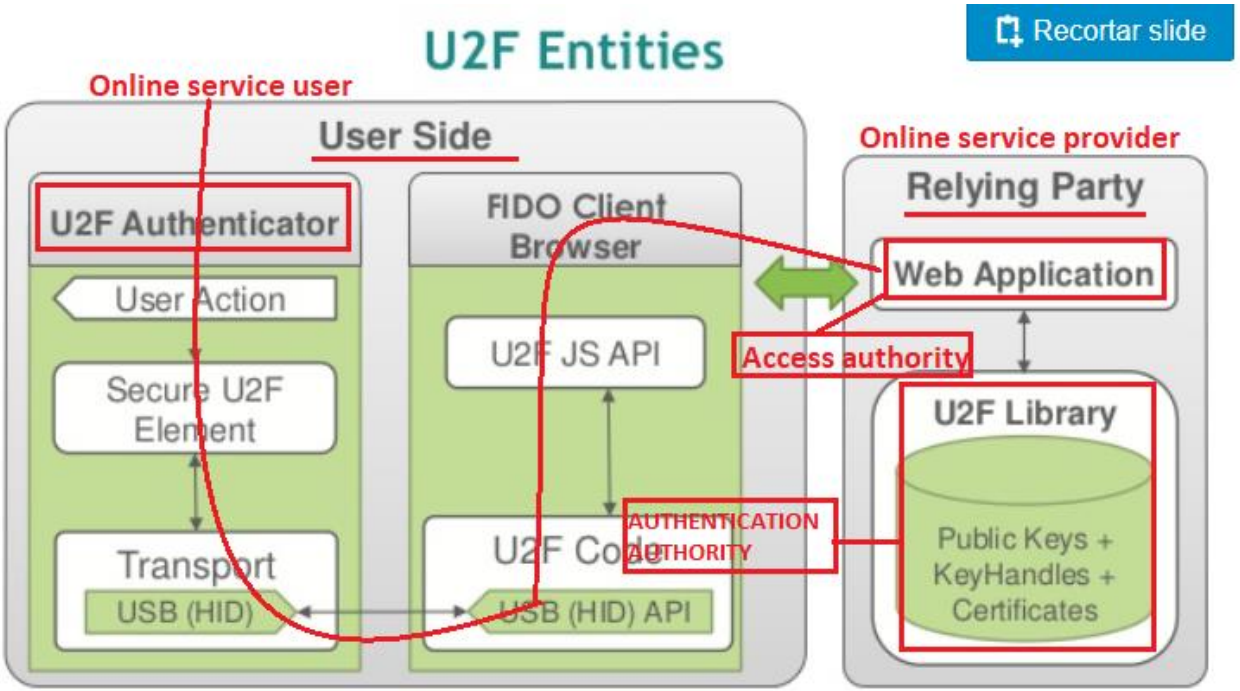
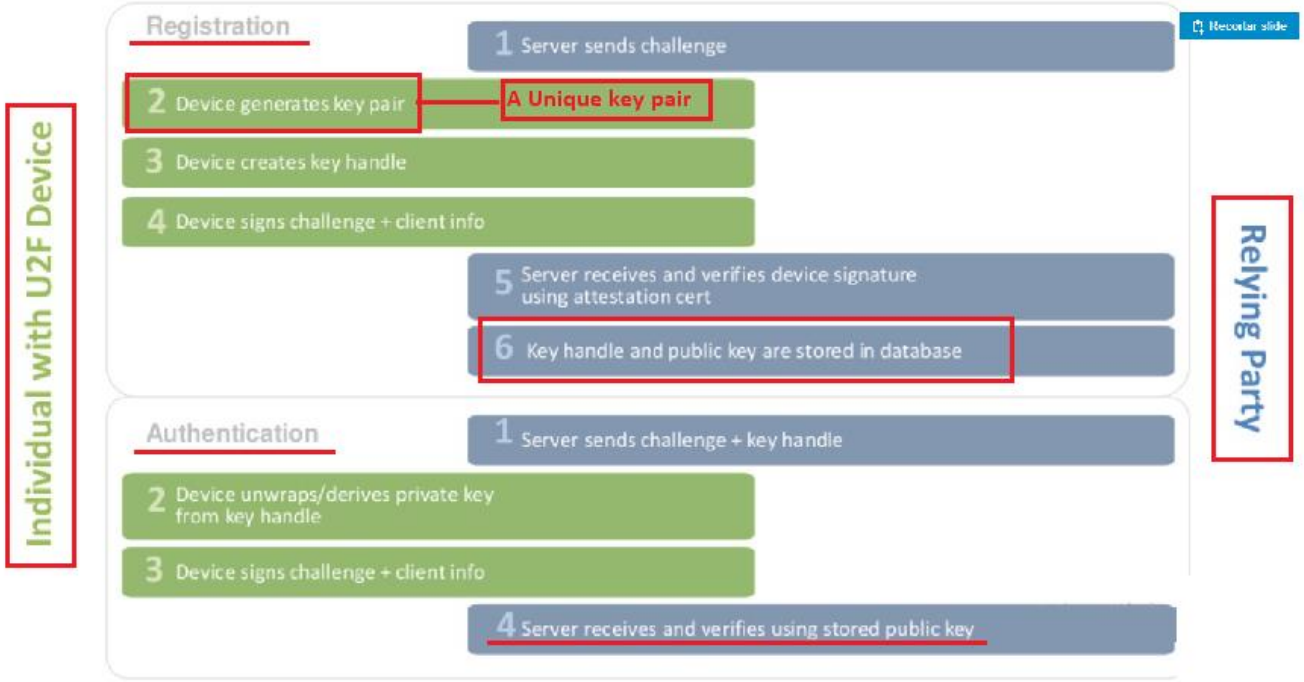
	 https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial
(ii) receiving a user ID, registration code, and suspect credentials,	The accused system practices receiving a user ID, registration code (e.g., passcode or PIN), and suspect credentials (e.g., public key (e.g., a first key) with the key handle). To use a U2F device in 2-factor authentication, a user (e.g., Individual with U2F device) has to register the U2F device with an authentication authority in the relying party. In the registration stage, the U2F device generates a unique key pair (A public key and a private key) and a key handle and sends the public key (e.g., a first key) with the handle to the authentication authority in the relying party to store them in its database of the relying party. The key pair is used to authenticate a suspected user by the authentication authority in the authentication stage.

EXHIBIT 2



https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial

EXHIBIT 2

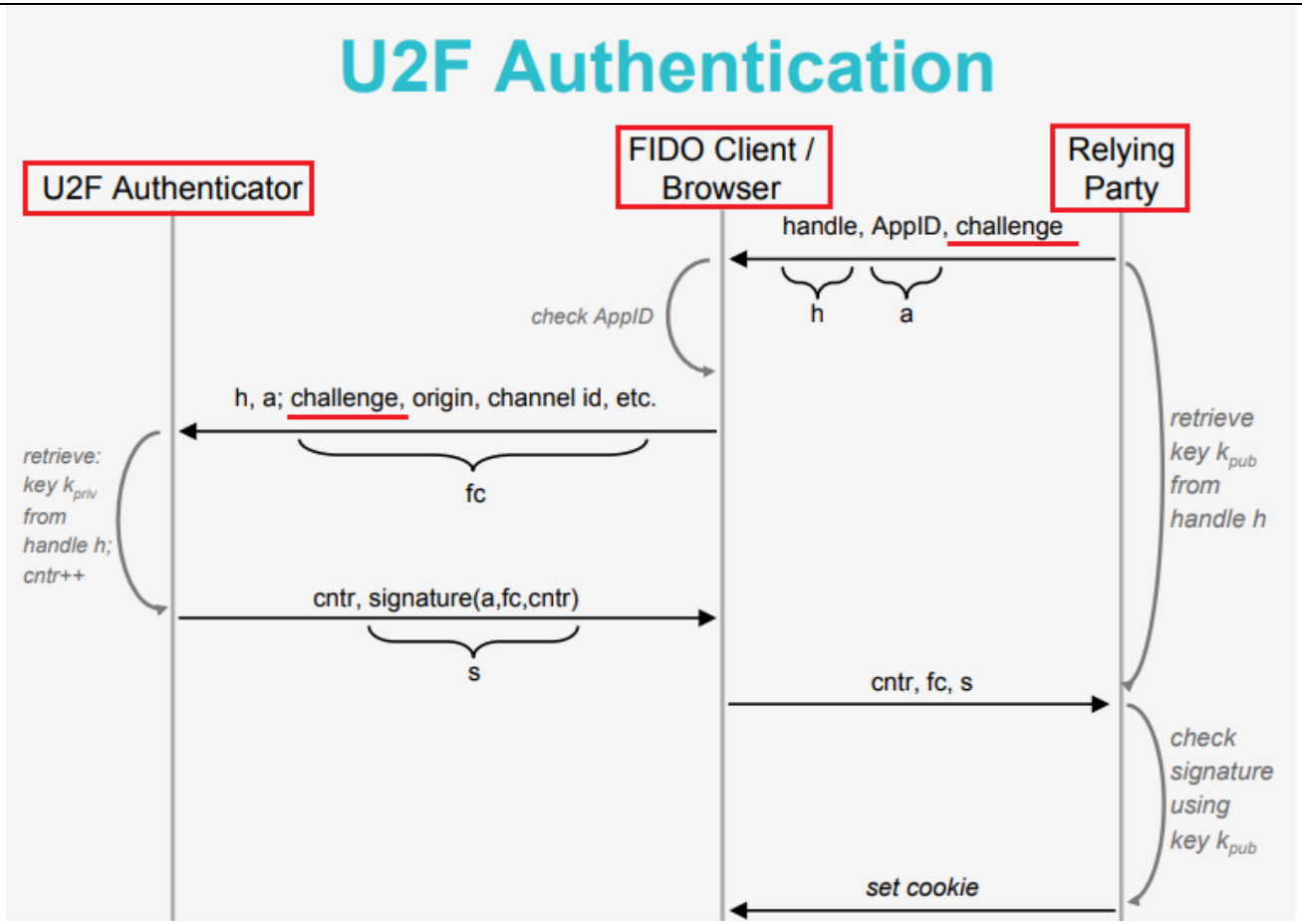
	 https://fidoalliance.org/assets/downloads/FIDO-U2F-UAF-Tutorial-v1.pdf
(iii) comparing the suspect credentials with the credentials maintained in association with the user ID, and	The accused system practices comparing the suspect credentials (e.g., public key (e.g., a first key) with the key handle) with the credentials maintained in association with the user ID. To use a U2F device in 2-factor authentication, a user (e.g., Individual with U2F device) has to register the U2F device with an authentication authority in the relying party. In the registration stage, the U2F device generates a unique key pair (A public key and a private key) and a key handle and sends the

EXHIBIT 2

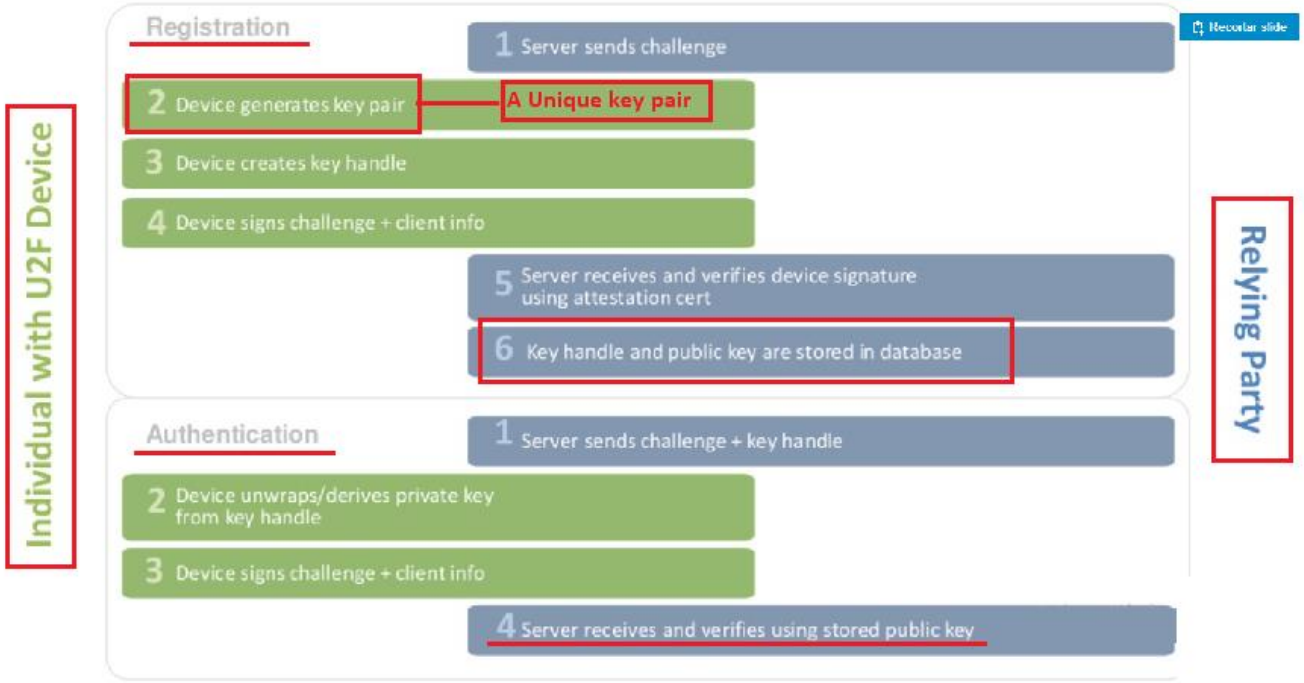
	public key (e.g., a first key) with the handle to the authentication authority in the relying party to store the them in its database of the relying party. The key pair is used to authenticate a suspected user by the authentication authority in the authentication stage.  https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial The following figure shows U2F database in the authentication authority in the relying party (e.g., online service provider) after the registration. The authentication authority maintains the public key (=a first key) of the key pair and the key handle generated by the U2F device and an identifier (=user_id), and the password (=a PIN) associated with it in its database. The U2F security key (authenticator) owned by the user maintains the private key of the key pair and the key handle (not shown).

EXHIBIT 2

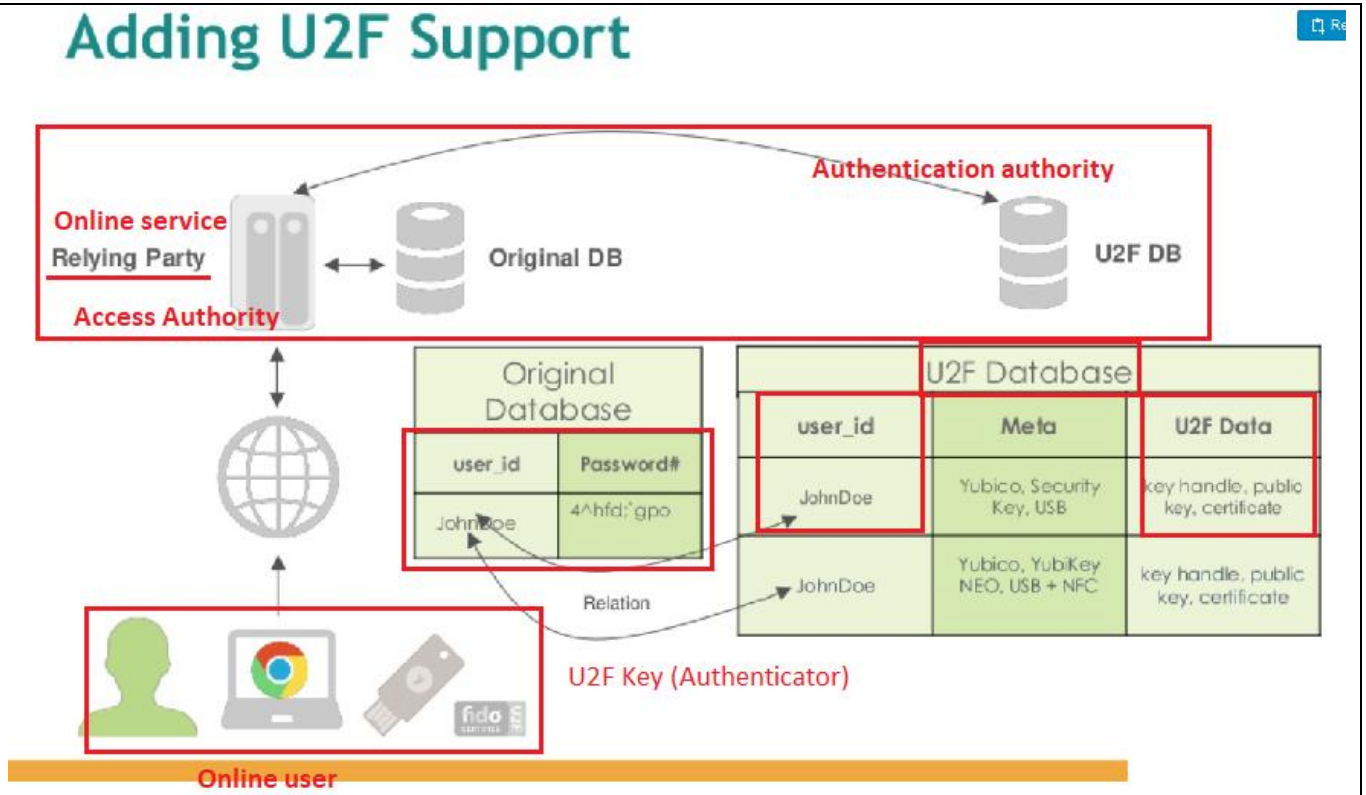
	 https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial
(iv) upon a successful authentication of the user ID by matching the suspect credentials with the maintained credentials, communicating the user ID and registration code to an authentication authority	The accused system practices communicating the user ID and registration code (e.g., passcode) to an authentication authority (e.g., U2F server with database in relying party) upon a successful authentication of the user ID by matching the suspect credentials (e.g., public key (a first key) with the key handle) with the maintained credentials. To use a U2F device in 2-factor authentication, a user (e.g., Individual with U2F device) has to register the U2F device with an authentication authority in the relying party. In the registration stage, the U2F device generates a unique key pair (A public key and a private key) and a key handle and sends the public key (e.g., a first key) with the handle to the authentication authority in the relying party to store

EXHIBIT 2

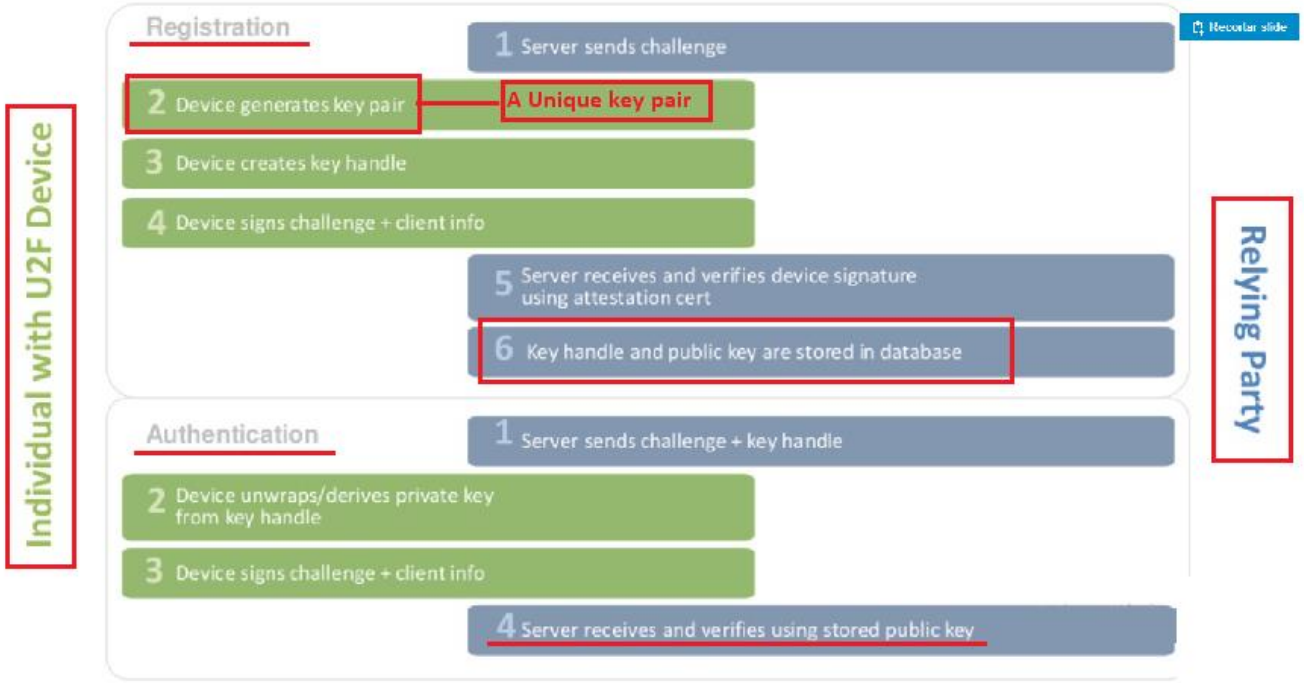
	the them in its database of the relying party. The key pair is used to authenticate a suspected user by the authentication authority in the authentication stage.  https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial

EXHIBIT 2

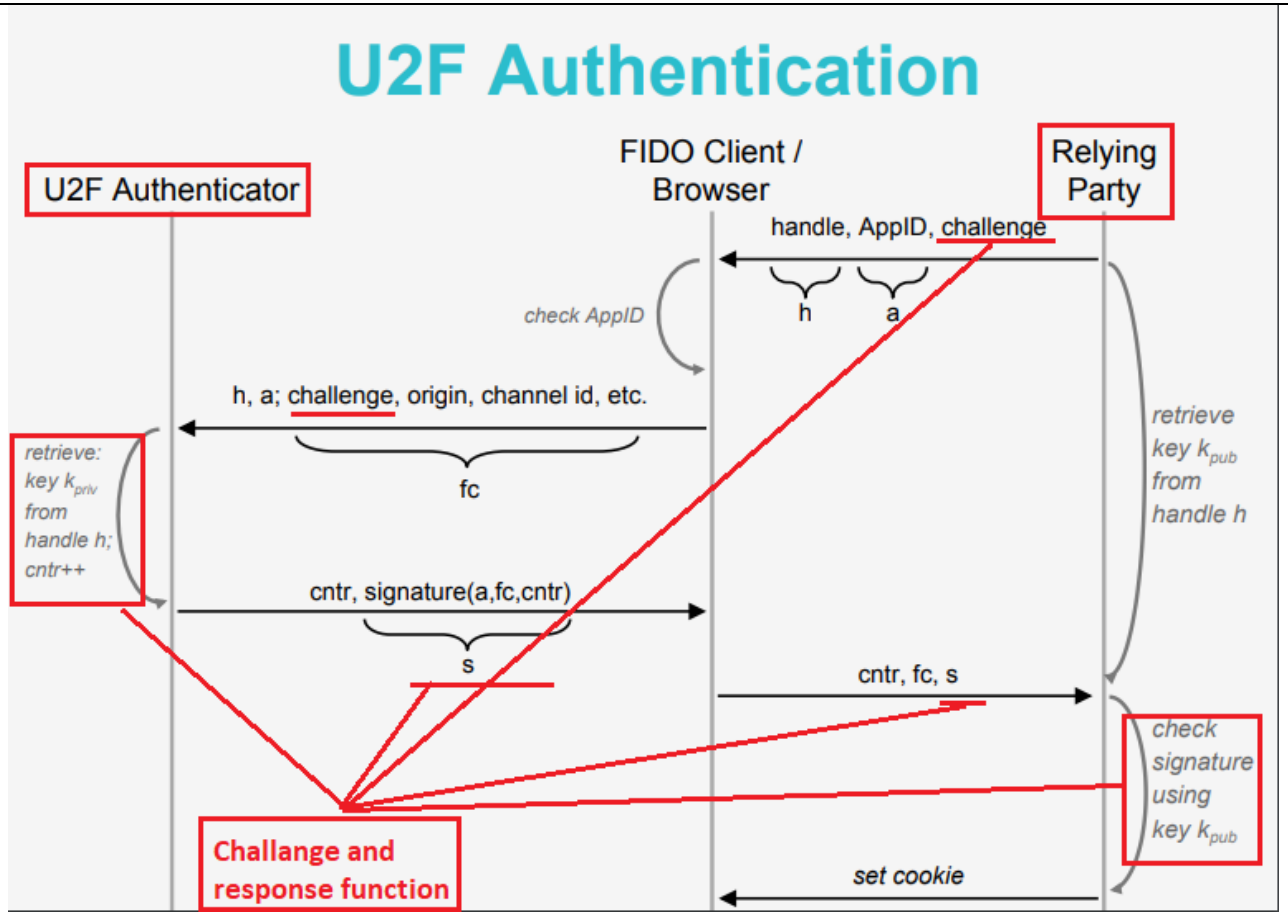
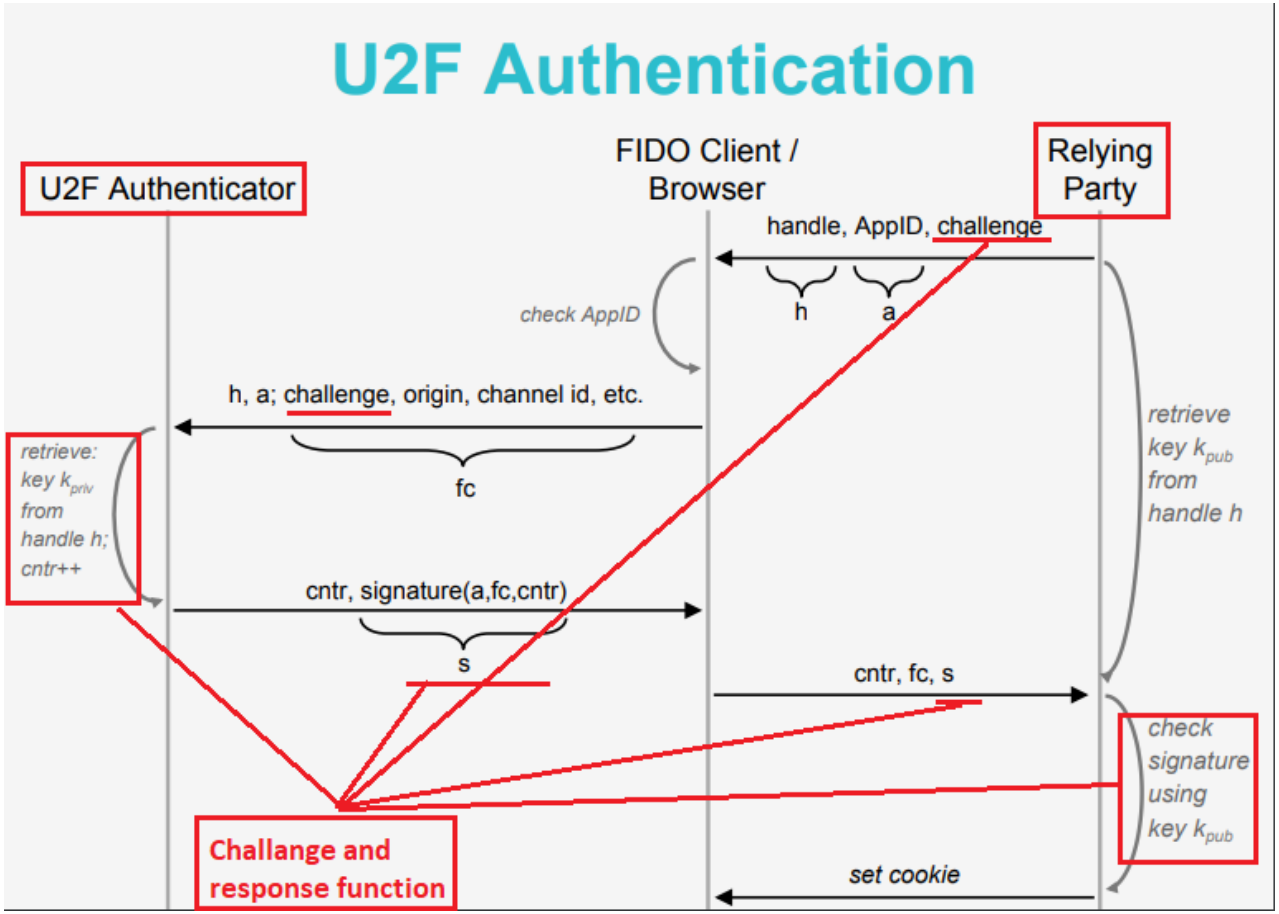
	 https://fidoalliance.org/assets/downloads/FIDO-U2F-UAF-Tutorial-v1.pdf
(b) thereafter, granting access to the network resource to a suspect user upon, (i) receiving a user ID and passcode from the suspect user,	The accused system practices granting access to the network resource (e.g., Online service like accused system) to a suspect user (e.g., an online user) upon receiving a user ID and passcode (e.g., PIN) from the suspect user. The authentication authority (in the relying party) verifies the identifier by using the challenge and response function.

EXHIBIT 2



https://fidoalliance.org/assets/downloads/FIDO-U2F-UAF-Tutorial-v1.pdf

To use a U2F device in 2-factor authentication, a user (e.g., Individual with U2F device) has to register the U2F device with an authentication authority in the relying party. In the registration stage, the U2F device generates a unique key pair (A public key and a private key) and a key handle and sends the public key (e.g., a first key) with the handle to the authentication authority in the relying party to store them in its database of the relying party. The key pair is used to authenticate a suspected user by the authentication authority in the authentication stage.

EXHIBIT 2

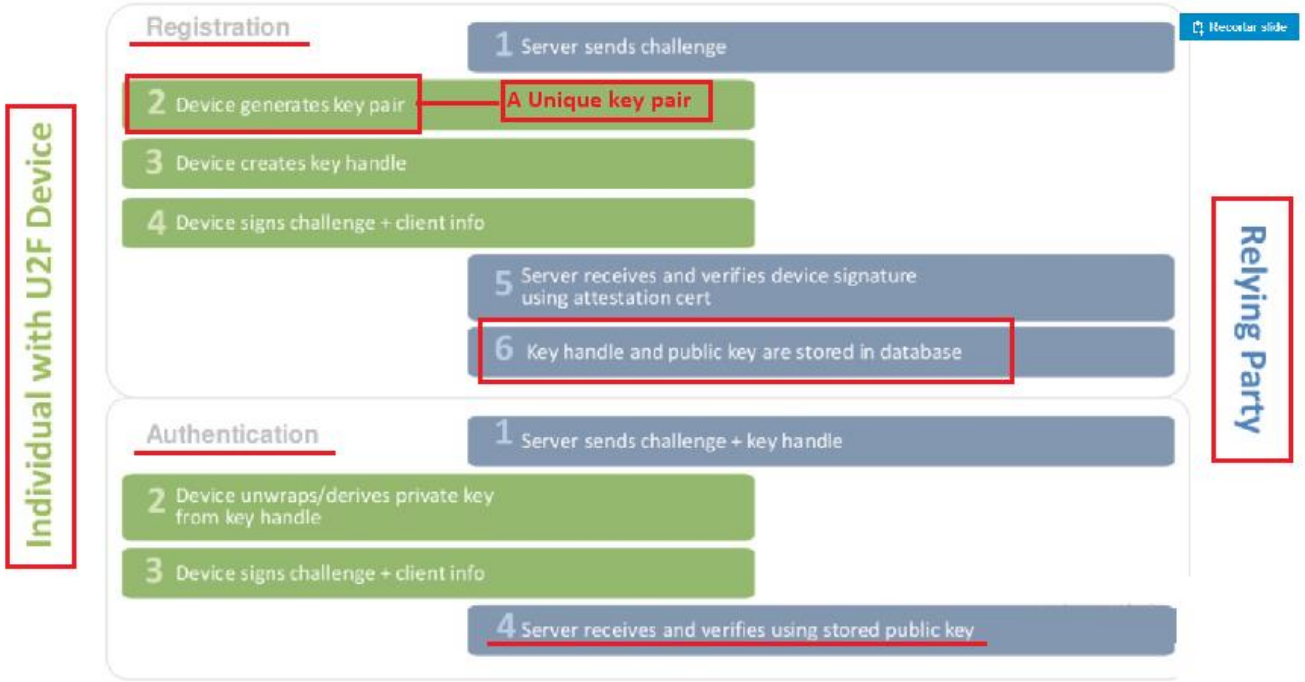
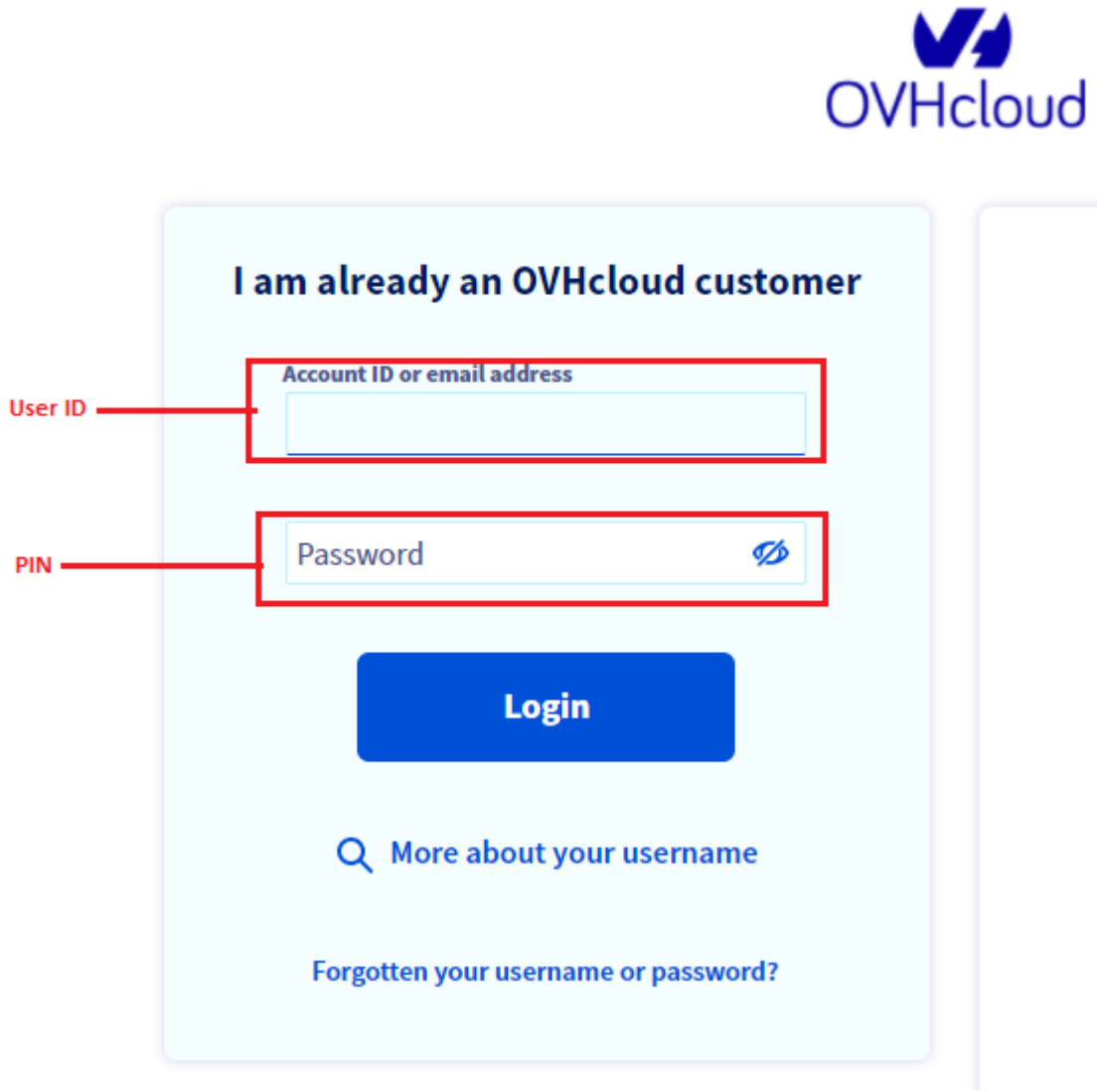
	 https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial
(ii) communicating the user ID and passcode to the authentication authority, and	The accused system practices communicating the user ID and passcode (e.g., password) to the authentication authority (e.g., U2F server with database). The authentication authority in the relying party like accused system also uses the password (=which is equal to a passcode) associated with user ID (=the identifier).

EXHIBIT 2



https://www.ovh.com/auth/?action=gotomanager&from=https://www.ovh.co.uk/&ovhSubsidiary=GB

EXHIBIT 2

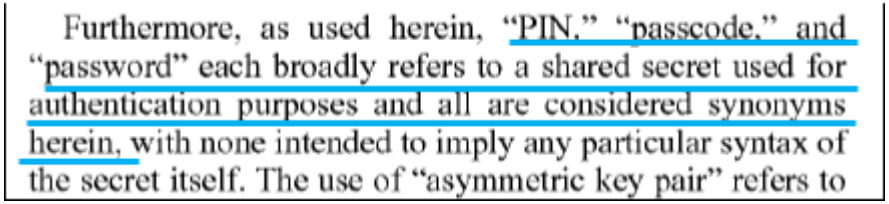
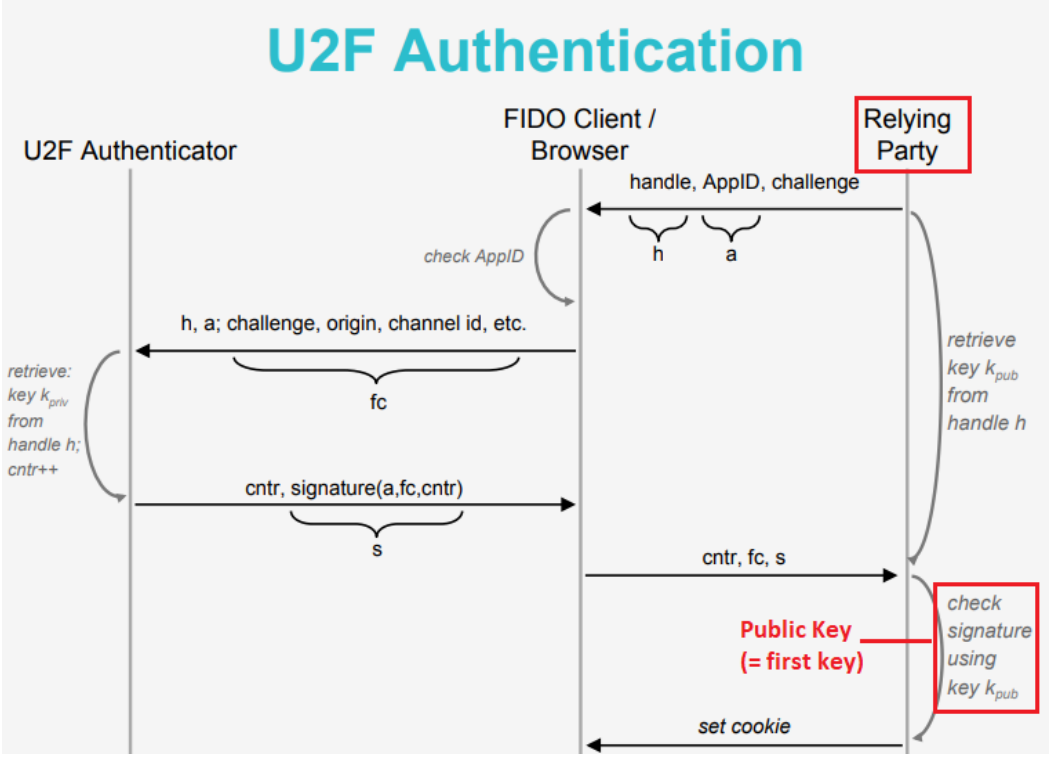
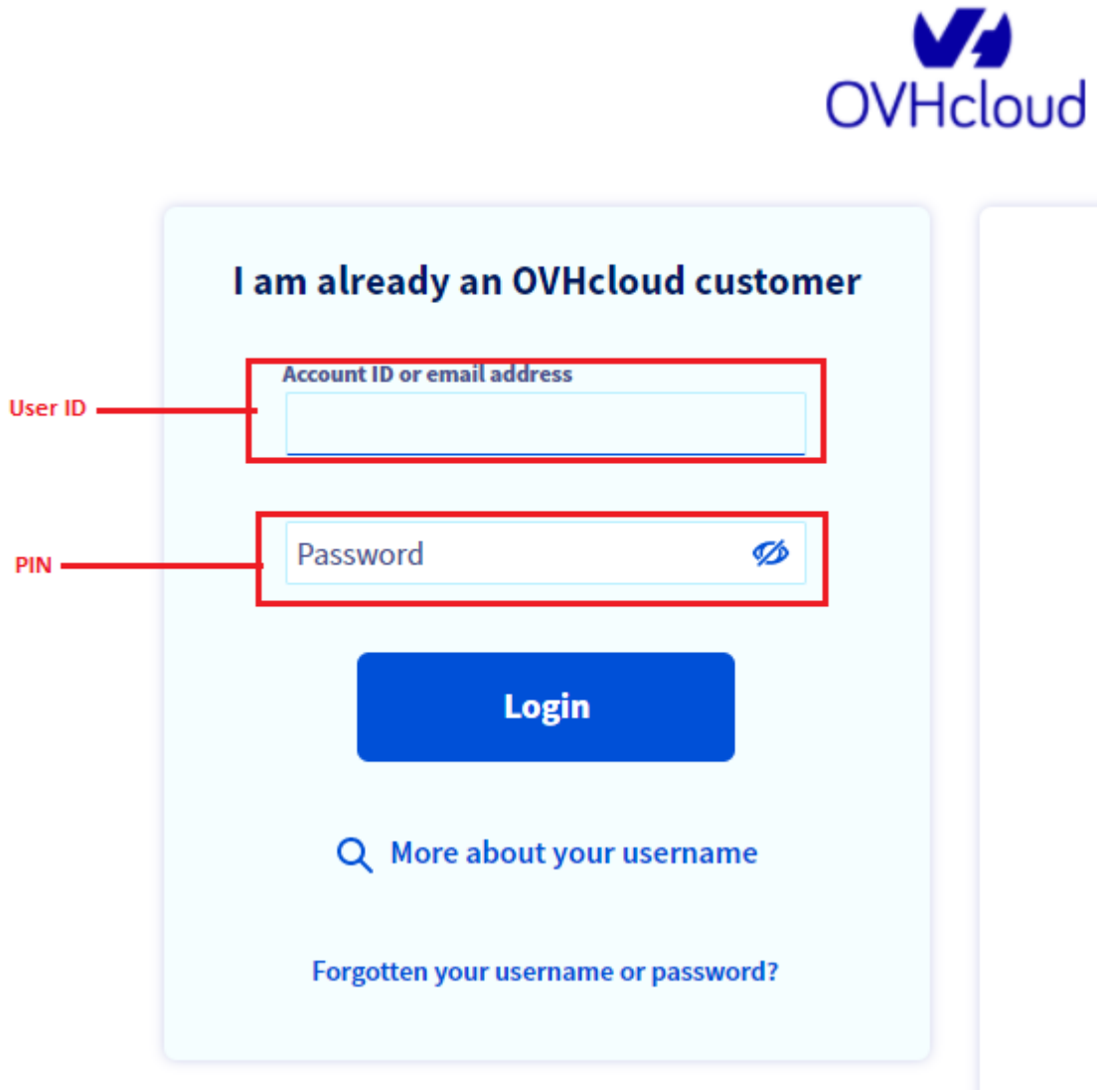
	PIN and password are synonyms according to the description of '515 patent shown below.  Furthermore, as used herein, "PIN," "passcode," and "password" each broadly refers to a shared secret used for authentication purposes and all are considered synonyms herein, with none intended to imply any particular syntax of the secret itself. The use of "asymmetric key pair" refers to https://patentimages.storage.googleapis.com/0d/08/49/2d86aa8d80d268/US7373515.pdf
(iii) receiving an indication of a successful passcode comparison by the authentication authority.	The accused system practices receiving an indication of a successful passcode (e.g., password) comparison by the authentication authority (e.g., U2F server with database in relying party). The authentication authority in the relying party verifies the signature received from the U2F authenticator associated with the identifier by decrypting the signature (s) with Kpub which is the public key (=the first key). If the challenge response is decoded successfully with the public key (=the first key) by the authentication authority, the U2F authenticator responds to the challenge is a trusted key.

EXHIBIT 2



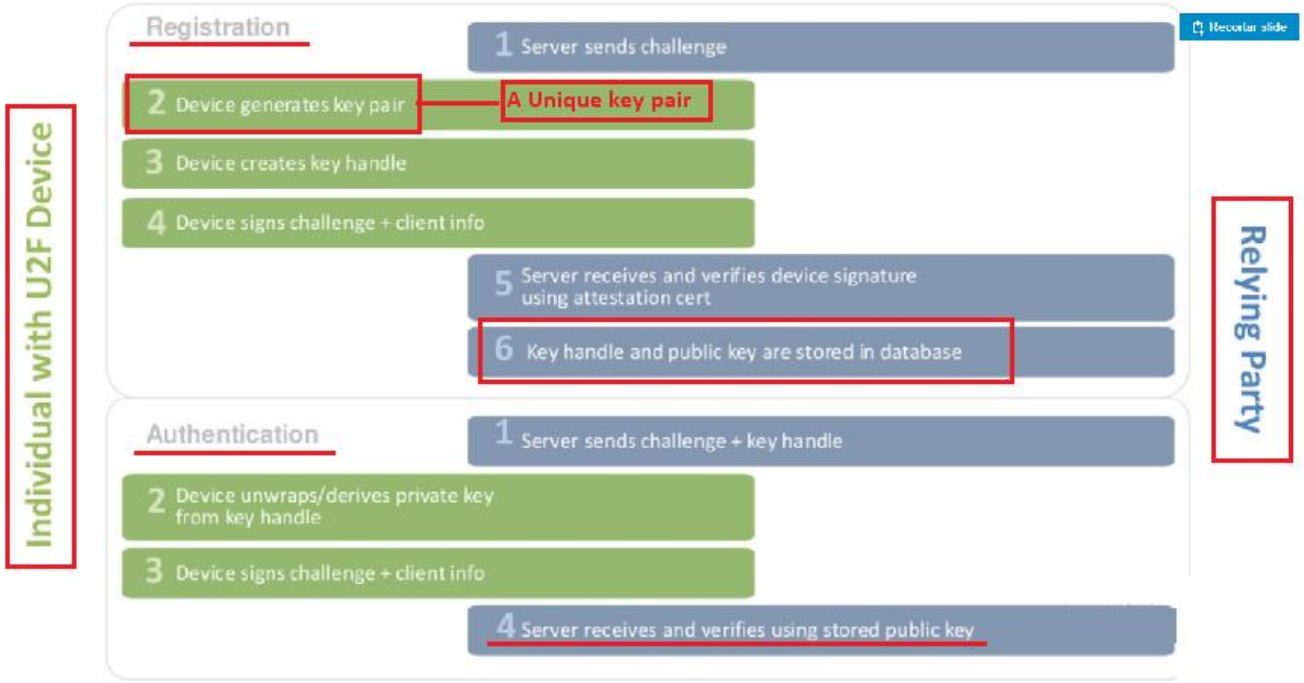
https://fidoalliance.org/assets/downloads/FIDO-U2F-UAF-Tutorial-v1.pdf

EXHIBIT 2



https://www.ovh.com/auth/?action=gotomanager&from=https://www.ovh.co.uk/&ovhSubsidiary=GB

EXHIBIT 2

	The key pair is used to authenticate a suspected user by the authentication authority in the authentication stage.  https://pt.slideshare.net/FIDOAlliance/fido-u2f-specifications-overview-tutorial